

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-145356

(43)Date of publication of application : 29.05.1998

(51)Int.Cl.

H04L 9/32

(21)Application number : 09-247133

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 11.09.1997

(72)Inventor : SHIMIZU AKIHIRO
HORIAKA TSUTOMU
HAMADA HIROSHI

(30)Priority

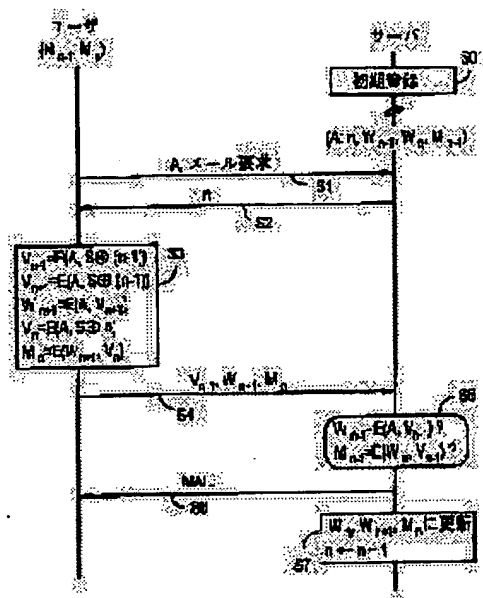
Priority number : 08240190 Priority date : 11.09.1996 Priority country : JP

(54) INFORMATION TRANSMITTING AND RECEIVING CONTROL METHOD WITH USER IDENTIFYING FUNCTION AND RECORDING MEDIUM RECORDING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To dispense with the read/write of a storing medium by the side of a person to be identified and to safely execute user identifying processing by a small program size by initially register the initial values and the identification A of identification data of this time and a time after next and its propriety inspecting data W_{n-1} , W_{n+1} and M_n , allowing both of a user and a server to calculate through the use of a unidirectional function each time of the identifying request of the user and identifying the user, when these data to increment match.

SOLUTION: E is the unidirectional function, and S is a password which the user holds secretly. (+) is exclusive OR. The user initially registers $V_0=E(A, S)$, $W_0=E(A, V_0)$, $V_1=E(A, S(+1))$, $W_1=E(A, V_1)$, $M_0=E(W_1, V_0)$. The server calculates $V_{n-1}=E(A, S(+)(n-1))$, $V_n=E(A, S(+)(n))$, $V_{n+1}=E(A, S(+)(n+1))$, $W_{n+1}=E(A, V_{n+1})$, $M_n=E(W_{n+1}, V_n)$ as an n-th identification value and compares it with a value received from the user.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C): 1998,2000 Japanese Patent Office

特開平 1 0 - 1 4 5 3 5 6

(43)公開日 平成 1 0 年 (1 9 9 8) 5 月 2 9 日

(51)Int.Cl.	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/32			H04L 9/00	675 A
				673 A
				673 C
				673 D

審査請求 未請求 請求項の数 2 0 O L (全 2 0 頁)

(21)出願番号	特願平 9 - 2 4 7 1 3 3	(71)出願人	0 0 0 0 0 4 2 2 6 日本電信電話株式会社 東京都新宿区西新宿三丁目 1 9 番 2 号
(22)出願日	平成 9 年 (1 9 9 7) 9 月 1 1 日	(72)発明者	清水 明宏 東京都新宿区西新宿三丁目 1 9 番 2 号 日 本電信電話株式会社内
(31)優先権主張番号	特願平 8 - 2 4 0 1 9 0	(72)発明者	堀岡 力 東京都新宿区西新宿三丁目 1 9 番 2 号 日 本電信電話株式会社内
(32)優先日	平 8 (1 9 9 6) 9 月 1 1 日	(72)発明者	浜田 洋 東京都新宿区西新宿三丁目 1 9 番 2 号 日 本電信電話株式会社内
(33)優先権主張国	日本 (J P)	(74)代理人	弁理士 草野 卓

(54)【発明の名称】 ユーザ認証機能を有する情報送受信制御方法及びその方法を記録した記録媒体

(57)【要約】

【課題】 被認証者側に記憶媒体の読み書きを行う機構を必要とせず、かつユーザ認証処理を小さいプログラムサイズで安全に行う。

【解決手段】 ユーザは $n=0$ 、メールアドレス A 、パスワード S を設定し、一方向性関数 $V_n = E(A, S)$ 、 $W_n = E(A, V_n)$ 、 $V_{n+1} = E(A, A(+1))$ 、 $W_{n+1} = E(A, V_{n+1})$ 、 $M_n = E(W_n, V_n)$ を求め、 W_n 、 V_n 、 M_n 、 A を電子メールでメールサーバに初期登録しておく。出先でユーザは電子メールにか加入している任意の端末を用い、サービス起動要求と A をメールサーバに送り、メールサーバは識別子 A の認証回数 n を読みだし、それを返送する。ユーザは $V_{n+1} = E(A, S(+)(n-1))$ 、 $V_{n+1} = E(A, S(+)(n+1))$ 、 $W_{n+1} = E(A, V_{n+1})$ 、 $V_n = E(A, S(+)(n))$ 、 $M_n = E(W_n, V_n)$ を求めて V_{n+1} 、 W_{n+1} 、 M_n をメールサーバに送る。メールサーバは、 $E(A, V_{n+1})$ 、 $E(W_n, V_{n+1})$ を求め、登録されているデータ W_{n+1} 、 M_{n+1} とそれぞれ一致すれば、OK としてそのユーザのメールメッセージを送る。

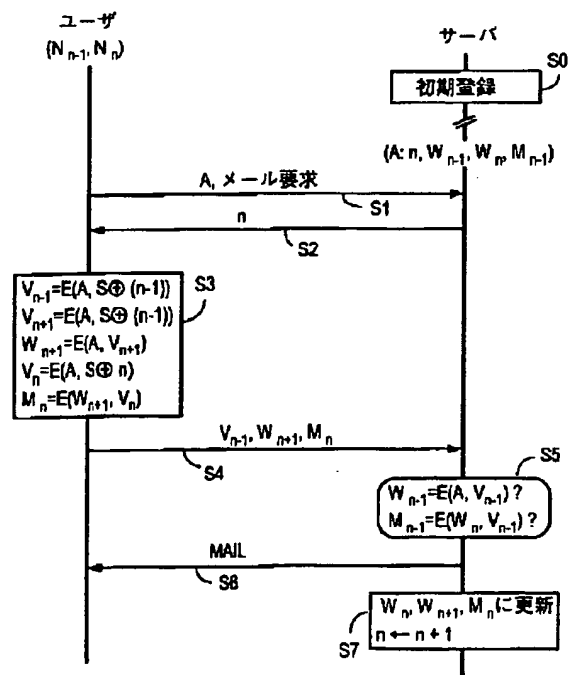


図 3

【特許請求の範囲】、

【請求項 1】 ネットワーク上でユーザが利用するユーザ端末装置と、認証者の認証者装置との間で認証処理を行うための情報送受信制御方法であり、以下のステップを含む：

(a) 初期登録手順として、上記ユーザが、自分の識別子 A と、秘密に保持しているパスワード S から、次回認証データ W_1 、次々回認証データ W_2 、上記次々回認証データ W_1 の正当性検証データ M_1 の 3 つを算出し、認証回数 n の初期値 $n=1$ と共に上記認証者装置に上記識別子 A と対応して登録し、

(b) 次に、 n を正の整数とすると、第 n 回目の認証において、上記認証者装置は、上記ユーザ端末装置からサービス起動要求と上記ユーザの識別子 A の通知を受けて、そのユーザの認証回数 n を読みだし、そのユーザ端末装置へ通知し、

(c) 上記ユーザ端末装置では、上記ユーザの識別子 A、送られてきた上記認証回数 n 及び秘密に保持しているパスワード S を用いて、今回の被認証データ V_{n+1} 、次々回の認証データ W_{n+1} 、次々回認証データ W_{n+1} の正当性検証データ M_{n+1} を算出し、送信したいコンテンツデータがある場合にはそのデータと共に上記認証者装置に通知し、

(d) 上記認証者装置では、上記ユーザの識別子 A と上記ステップ (c) で送付されてきた今回の被認証データ V_{n+1} とから算出した今回の認証データ W_{n+1} を、登録されている認証データ W_n と比較し、かつ登録されている次回認証データ W_{n+2} と、上記今回の被認証データ V_{n+1} とから計算した正当性検証データ M_{n+1} を、登録されている正当性検証データ M_n と比較し、

(e) 上記ステップ (d) の比較の結果、一致した場合、上記認証者装置ではそのユーザを正当とし、上記ユーザが要求したサービス情報の送受信を行うとともに、前回受けた次回認証データ W_n と、今回送付されてきた次々回認証データ W_{n+1} と、次々回認証データの正当性検証データ M_{n+1} を、前回登録した W_{n-1} 、 W_n 、 M_n と置き換えて登録し、認証回数 n をインクリメントし、

(f) 上記ステップ (d) の比較の結果、一致しない場合、そのユーザを不当とし以降の情報送受信を拒否し、前回登録したデータ W_{n-1} 、 W_n 、 M_n 及び n をそのまま保持する。

【請求項 2】 請求項 1 の方法において、上記ユーザは上記認証者装置において上記ステップ (a) の初期登録手順を実行する。

【請求項 3】 請求項 1 の方法において、上記ユーザ端末装置と認証者装置間のデータ送受信に、電子メールプロトコルを用い、通信処理のコンテンツデータを上記ユーザ宛の電子メールとし、認証者装置にある上記ユーザの電子メール情報を遠隔地にある上記ユーザ端末装置へ転送したり、あるいは、上記ユーザのメールアドレスで遠隔地から電子メールの発信を行う。

【請求項 4】 請求項 1 の方法において、上記ユーザは、上記ユーザ端末装置において上記データ W_1 、 W_2 、 M_1 を生成し、上記認証回数初期値 $n=1$ と共に上記認証者装置に送信することにより上記ステップ (a) の初期登録手順を実行する。

【請求項 5】 請求項 4 の方法において、上記認証者装置は、上記ステップ (b) において上記ステップ (c) のユーザ側認証手順を特定の通信単位に予め決められた方法で記述したプログラムの通信単位を上記ユーザ端末装置へ送り込み、上記ステップ (c) において上記ユーザ端末装置はその送り込まれた通信単位プログラムを実行することにより認証手順を実行する。

【請求項 6】 請求項 4 の方法において、上記認証者装置は、上記ステップ (a) の前にユーザの要求に応じて上記ステップ (a) の初期登録手順を特定の通信単位に予め決められた方法で記述したプログラムの通信単位を上記ユーザ端末装置へ送り込み、上記ステップ (a) において上記ユーザ端末装置はその通信単位プログラムを実行することにより上記初期登録手順を実行する。

【請求項 7】 請求項 1 又は 4 の方法において、(f) を排他的論理和、E を一方向性関数とすると、上記ステップ (a) は次の手順

$$V_1 = E(A, S)$$

$$W_1 = E(A, V_1)$$

$$V_2 = E(A, S(+1))$$

$$W_2 = E(A, V_2)$$

$$M_1 = E(W_1, V_1)$$

で上記データ初期値 W_1 、 W_2 、 M_1 を算出し、上記ステップ (c) は次の手順

$$V_{n+1} = E(A, S(+)(n-1))$$

$$V_n = E(A, S(+)(n))$$

$$V_{n+1} = E(A, S(+)(n+1))$$

$$W_{n+1} = E(A, V_{n+1})$$

$$M_n = E(W_n, V_n)$$

で上記認証用データ V_{n+1} 、 W_{n+1} 、 M_{n+1} を算出し、上記ステップ (d) は上記ユーザから受信したデータ V_{n+1} と、登録されているデータ A、 W_n とから $E(A, V_{n+1})$ と $E(W_n, V_{n+1})$ を計算し、それらが登録されているデータ W_{n+1} と M_{n+1} にそれぞれ一致するかを判定する。

【請求項 8】 請求項 1 の方法において、上記ネットワークは上記ユーザ端末装置が接続されたインターネットと、そのインターネットに接続されたイントラネットを含み、上記認証者装置は上記イントラネット上に接続して設けられており、上記インターネット上に公開された中継サーバが接続して設けられており、上記ユーザと上記中継サーバの間では高速通信プロトコルを使って送受信が行われ、上記中継サーバと上記認証装置の間では電子メールプロトコルを使って送受信が行われ、それによって、上記ユーザ端末装置と上記認証装置間での認証情報のやりとりを上記中継サーバを介して行う。

【請求項 9】 請求項 8 の方法において、上記ユーザは上記ステップ(c)において上記データ V_{n+1} , W_{n+1} , M_n を送出後、一旦上記中継サーバとの接続を切断し、上記認証者装置は上記ステップ(e)において認証が完了した時点で、上記ユーザが要求したサービスの情報を上記中継サーバに転送し、そこに保管し、上記ユーザは、上記中継サーバとの接続を切断してから一定時間が経過した後の任意の時間に上記中継サーバに再度接続し、上記中継サーバとの間で上記サービス情報に対する上記ユーザの正当性を検証する認証処理を行い、上記サービス情報を受信する。

【請求項 10】 インタネットにユーザ端末装置と中継サーバがそれぞれ接続されており、そのインタネットに接続されたイントラネットに認証者装置が接続されており、上記ユーザ端末装置と上記認証者装置との間の情報送受信を上記中継サーバを介して行う場合に、上記ユーザ端末装置と上記中継サーバ間は高速通信プロトコルを使って行い、上記中継サーバと上記認証者装置間は電子メールプロトコルを使って行うシステムにおける、上記ユーザと認証者との間で認証処理を行うための情報送受信制御方法であり、以下のステップを含む：

(a) 上記ユーザの識別子 A と、秘密に保持しているパスワード S から、次回認証データ W_0 、次々回認証データ W_1 、上記次々回認証データ W_i の正当性検証データ M_0 の 3 つを算出し、上記認証者装置に上記識別子 A と対応して登録し、上記認証回数 n の初期値 $n=1$ を上記認証者装置と上記中継サーバにそれぞれ上記識別子 A と対応させて保持し、

(b) n を正の整数とすると、第 n 回目の認証において、上記中継サーバは上記ユーザ端末装置からサービス要求と識別子 A を受けると、対応する認証回数 n を読みだし、上記ユーザ端末装置に送り、

(c) 上記ユーザ端末装置では、上記ユーザの識別子 A 、送られてきた上記認証回数 n 及び秘密に保持しているパスワード S を用いて、今回の被認証データ V_{n+1} 、次々回の認証データ W_{n+1} 、その次々回認証データ W_{n+1} の正当性検証データ M_{n+1} を算出し、送信したいコンテンツデータがある場合にはそのデータと共に上記中継サーバを介して上記認証者装置に送り、その後上記中継サーバとの接続を一旦切断し、

(d) 上記認証者装置では、上記ユーザの識別子 A と上記ステップ(c)で送付されてきた今回の被認証データ V_{n+1} とから算出した今回の認証データ W_{n+1} を、登録されている認証データ W_{n+1} と比較し、かつ登録されている次回認証データ W_n と、上記今回の被認証データ V_{n+1} とから計算した正当性検証データ M_{n+1} を、登録されている正当性検証データ M_{n+1} と比較し、

(e) 上記ステップ(d)の比較の結果、一致した場合、上記認証者装置では、そのユーザを正当とし、上記ユーザが要求したサービスの情報を上記中継サーバに転送し

て、そこに保管し、或いは、送信したいコンテンツ情報がある場合には、認証されたユーザの資格でその情報の送信を行い、送信を完了したことを示す確認情報を中継サーバに送信し、

(f) 上記認証者装置は更に、前回受けた次回認証データ W_n と、今回送付されてきた次々回認証データ W_{n+1} と、次々回認証データの正当性検証データ M_n を、前回登録したデータ W_{n-1} , W_n , M_{n-1} と置き換えて登録し、認証回数 n をインクリメントし、上記ステップ(d)の比較の結果、一致しない場合、そのユーザを不当とし以降の情報送受信を拒否し、前回登録した W_{n-1} , W_n , M_n 及び n をそのまま保持し、

(g) 上記中継サーバは、上記サービス情報或いは上記送信確認情報を受け取った後、上記認証回数 n をインクリメントし、

(h) 上記ユーザは、上記中継サーバとの接続を切断してから一定時間が経過した後の任意の時間に上記中継サーバに再度接続し、上記中継サーバとの間で上記サービス情報に対する上記ユーザの正当性を検証する認証処理を行い、上記サービス情報を受信する。

【請求項 11】 請求項 9 又は 10 の方法において、

(+) を排他的論理和、 E を一方向性関数、上記認証者装置の識別子を A_n とすると、上記ステップ(a)では上記初期登録のための上記 3 つのデータ W_0 , W_1 , M_0 を次の手順
 $V_0 = E(A(+)A_n, S)$
 $W_0 = E(A(+)A_n, V_0)$
 $V_1 = E(A(+)A_n, S(+1))$
 $W_1 = E(A(+)A_n, V_1)$
 $M_0 = E(W_1, V_0)$

により求め、上記ユーザは上記第 n 回目の認証における上記データ V_{n+1} , W_{n+1} , M_{n+1} を次の手順

$V_{n+1} = E(A(+)A_n, S(+)(n-1))$
 $V_n = E(A(+)A_n, S(+)(n))$
 $V_{n+1} = E(A(+)A_n, S(+)(n+1))$
 $W_{n+1} = E(A(+)A_n, V_{n+1})$
 $M_n = E(W_{n+1}, V_n)$

により求め、上記認証者装置は上記比較をする処理を $W_{n+1} = E(A(+)A_n, V_{n+1})$ の一致と、 $M_{n+1} = E(W_{n+1}, V_n)$ の一致を検証することによって行う。

【請求項 12】 請求項 11 の方法において、上記ユーザと上記中継サーバ間の認証は、その認証回数を n' とし、上記中継サーバの識別子を A_n とすると、以下のステップを含む：

(a') 初期登録手順として、上記ユーザが、一方向性関数 E を使って自分の識別子 A と、秘密に保持しているパスワード S から、次回認証データ W_0 、次々回認証データ W_1 、次々回認証データ W_i の正当性検証データ M_0 の 3 つを算出し、認証回数 n' の初期値 $n'=1$ と共に上記中継サーバに上記識別子 A と対応して登録し、

(b') 次に、 n' を正の整数とすると、第 n' 回目の認

証において、上記中継サーバは、上記ユーザ端末装置からサービス要求と上記ユーザの識別子 A の通知を受けて、そのユーザの認証回数 n' を読みだし、そのユーザ端末装置へ通知し、

(c') 上記ユーザ端末装置では、上記ユーザの識別子 A、送られてきた上記認証回数 n' 及び秘密に保持しているパスワード S を用いて、今回の被認証データ $V_{n'}$ 、次々回の認証データ $W_{n'+1}$ 、次々回認証データ $W_{n'+2}$ の正当性検証データ $M_{n'+1}$ を算出し、

(d') 上記中継サーバでは、上記ユーザの識別子 A と上記ステップ (c') で送付されてきた今回の被認証データ $V_{n'}$ とから算出した今回の認証データ $W_{n'}$ を、登録されている認証データ $W_{n'-1}$ と比較し、かつ登録されている次回認証データ $W_{n'}$ と、上記今回の被認証データ $V_{n'}$ とから計算した正当性検証データ $M_{n'}$ を、登録されている正当性検証データ $M_{n'-1}$ と比較し、

(e') 上記ステップ (d') の比較の結果、一致した場合、そのユーザを正当とし、上記ユーザが要求したサービスの情報送受信を行うとともに、前回受けた次回認証データ $W_{n'}$ と、今回送付されてきた次々回認証データ $W_{n'+1}$ と次々回認証データの正当性検証データ $M_{n'+1}$ を、前回登録した $W_{n'-1}$ 、 $W_{n'}$ 、 $M_{n'}$ と置き換えて登録し、認証回数 n' をインクリメントする。

【請求項 13】 請求項 12 の方法において、上記ステップ (a') は上記次回認証データ W_n 、次々回認証データ W_{n+1} 、次々回認証データ W_{n+2} の正当性検証データ M_n を次式

$$V_n = E(A(+)A_n, S)$$

$$W_n = E(A(+)A_n, V_n)$$

$$V_{n+1} = E(A(+)A_n, S(+)1)$$

$$W_{n+1} = E(A(+)A_n, V_{n+1})$$

$$M_n = E(W_n, V_n)$$

により計算し、上記ステップ (b') は上記今回の被認証データ $V_{n'}$ 、次々回の認証データ $W_{n'+1}$ 、次々回認証データ $W_{n'+2}$ の正当性検証データ $M_{n'+1}$ を次式

$$V_{n'+1} = E(A(+)A_n, S(+) (n'-1))$$

$$V_{n'+2} = E(A(+)A_n, S(+) n')$$

$$V_{n'+3} = E(A(+)A_n, S(+) (n'+1))$$

$$W_{n'+1} = E(A(+)A_n, V_{n'+1})$$

$$M_{n'+1} = E(W_{n'+1}, V_{n'+1})$$

により計算し、上記ステップ (d') は今回の認証データ $W_{n'}$ 、 $W_{n'+1}$ 、 $W_{n'+2}$ を、登録されている認証データ $W_{n'-1}$ と比較し、かつ登録されている次回認証データ $W_{n'}$ と、上記今回の被認証データ $V_{n'}$ とから計算した正当性検証データ $M_{n'}$ 、 $M_{n'+1}$ 、 $M_{n'+2}$ を、登録されている正当性検証データ $M_{n'-1}$ と比較する。

【請求項 14】 ユーザ端末装置と、サービスプロバイダと、認証者装置とがインターネットに接続されており、ユーザがインターネット上でサービスプロバイダからサービスを受ける場合に、ユーザが認証者装置との間で認証処理を行うための情報送受信制御方法であり、以下のス

テップを含む：

(a) 初期登録手順として、上記ユーザのアカウント A と、パスワード S から次回認証データ W_n 、次々回認証データ W_{n+1} 、上記次々回認証データ W_{n+2} の正当性検証データ M_n の 3 つを計算し、認証回数初期値 $n=1$ と、金額 X と共に上記アカウント A と対応して登録し、

(b) ユーザは上記サービスプロバイダに所望のサービスを要求するサービス要求信号とアカウント A を送り、

(c) 上記サービスプロバイダは受信した上記アカウント A を上記課金管理センタに転送し、

(d) 上記課金管理センタは上記アカウント A に対応する認証回数 n を読み出し、上記サービスプロバイダに送り、

(e) 上記サービスプロバイダは受信した認証回数 n を認証手順の Applet プログラムと共にユーザ端末装置に送り、

(f) 上記ユーザは上記認証手順に従って認証用データ $V_{n'}$ 、 $W_{n'+1}$ 、 $M_{n'+1}$ を計算し、上記アカウント A と共に上記サービスプロバイダに送り、

(g) 上記サービスプロバイダはデータ $V_{n'}$ 、 $W_{n'+1}$ 、 $M_{n'+1}$ と共に上記サービスプロバイダのアカウント A_n と、上記サービスに対する金額 x を上記課金管理センタに送り、

(h) 上記認証者装置は上記サービス金額 x が上記アカウント A に対応して登録されている残額 X 以下であることを確認し、受信したデータ $V_{n'}$ と登録されている次回認証データ W_n を検証し、両方とも正しければ認証確認信号 OK を上記サービスプロバイダに送ると共に、データ W_n 、 W_{n+1} 、 M_n に更新し、認証回数 n をインクリメントし、上記アカウント A の残額 X を $X-x$ で更新し、上記プロバイダのアカウント A_n の残額 XP を X_n+x で更新し、

(i) 上記サービスプロバイダは、上記確認信号 OK を受けると上記ユーザに上記指定されたサービスを提供する。

【請求項 15】 ネットワーク上でユーザの正当性を認証するための情報送受信制御を行う認証者装置であり、以下を含む： n を正の整数とすると、次回認証データ $W_{n'}$ 、次々回認証データ $W_{n'+1}$ 、上記次々回認証データ $W_{n'+2}$ の正当性検証データ $M_{n'+1}$ を認証回数 n と共に上記識別子 A と対応して第 $n-1$ 回目の認証時に登録した登録データ記憶手段と、

第 n 回目の認証において、上記ユーザの端末装置からサービス起動要求と上記ユーザの識別子 A の通知を受けて、そのユーザの認証回数 n を上記登録データ記憶手段から読みだし、そのユーザ端末装置へ通知する認証回数送出手段と、

上記ユーザ端末装置から送られてきた今回の被認証データ $V_{n'}$ 、次々回の認証データ $W_{n'+1}$ 、上記次々回認証データ $W_{n'+2}$ の正当性検証データ $M_{n'+1}$ を受信する受信手段と、

上記ユーザの識別子 A と上記受信した今回の被認証データ $V_{n'}$ とから算出した今回の認証データ $W_{n'}$ を、上記登録データ記憶手段に登録されている認証データ $W_{n'-1}$ と比

較し、かつ登録されている次回認証データ W_{i+1} と、上記今回の被認証データ V_{i+1} とから計算した正当性検証データ M_{i+1} を、登録されている正当性検証データ M_{i+1} と比較する認証手段と、及び上記認証手段による比較の結果、一致した場合、そのユーザを正当とし、登録されている次回認証データ W_{i+1} と、今回受信した次々回認証データ W_{i+1} と、及び今回受信した次々回認証データの正当性検証データ M_{i+1} とを、上記登録データ記憶手段に登録されているデータ W_{i+1} 、 W_{i+1} 、 M_{i+1} と置き換えて登録し、認証回数 n をインクリメントする登録更新手段。

【請求項 16】 請求項 15 の装置において、上記認証手段は、上記ユーザから受信したデータ V_{i+1} と、登録されているデータ A 、 W_{i+1} とから一方向性関数 $E(A, V_{i+1})$ と $E(W_{i+1}, V_{i+1})$ を計算し、それらが登録されているデータ W_{i+1} と M_{i+1} にそれぞれ一致するかを判定する手段を含む。

【請求項 17】 ネットワーク上で認証者からユーザに対する認証得るための情報送受信制御を行うユーザ端末装置であり、以下を含む：認証者装置から認証回数 n を受信する認証回数受信手段と、

上記ユーザの識別子 A 、受信した上記認証回数 n 及び秘密に保持しているパスワード S を用いて、今回の被認証データ V_{i+1} 、次々回の認証データ W_{i+1} 、上記次々回認証データ W_{i+1} の正当性検証データ M_{i+1} をそれぞれ認証用データとして計算する認証用データ計算手段と、
上記認証用データを上記認証者装置に送信する認証用データ送信手段。

【請求項 18】 請求項 17 の装置において、(+) を排他的論理和とすると、上記認証用データ計算手段は、次の一方向性関数

$$V_{i+1} = E(A, S(+)(n-1))$$

$$V_i = E(A, S(+)(n))$$

$$V_{i+1} = E(A, S(+)(n+1))$$

$$W_{i+1} = E(A, V_{i+1})$$

$$M_{i+1} = E(W_{i+1}, V_{i+1})$$

により上記認証用データ V_{i+1} 、 W_{i+1} 、 M_{i+1} を算出する手段である。

【請求項 19】 ネットワーク上でユーザの正当性を認証する認証者側の認証手順を記録した記録媒体であり、上記認証手順は以下を含む：

(a) (+) を排他的論理和とすると、ユーザの識別子 A とパスワード S を使って次の一方向性関数

$$V_i = E(A, S)$$

$$W_i = E(A, V_i)$$

$$V_{i+1} = E(A, S(+)(1))$$

$$W_{i+1} = E(A, V_{i+1})$$

$$M_{i+1} = E(W_{i+1}, V_{i+1})$$

によりデータ初期値 W_i 、 W_{i+1} 、 M_{i+1} を算出して登録し、

(b) n を正の整数とすると、第 n 回目の認証において、上記ユーザの端末装置からサービス起動要求と上記ユー

ザの識別子 A の通知を受けて、そのユーザの認証回数 n を上記登録データ記憶手段から読みだし、そのユーザ端末装置へ送信し、

(c) 上記ユーザ端末装置から送られてきた今回の被認証データ V_{i+1} 、次々回の認証データ W_{i+1} 、その次々回認証データ W_{i+1} の正当性検証データ M_{i+1} を受信し、

(d) 上記ユーザの識別子 A と上記受信した今回の被認証データ V_{i+1} とから一方向性関数 $W_{i+1} = E(A, V_{i+1})$ により今回の認証データ W_{i+1} を算出し、上記登録データ記憶手段に登録されている認証データ W_{i+1} と比較し、かつ登録されている次回認証データ W_{i+1} と、上記今回の被認証データ V_{i+1} とから一方向性関数 $M_{i+1} = E(W_{i+1}, V_{i+1})$ により正当性検証データ M_{i+1} を算出し、登録されている正当性検証データ M_{i+1} と比較し、

(e) 2つの比較結果が同時に一致であった場合、そのユーザを正当とし、登録されている次回認証データ W_{i+1} と、今回受信した次々回認証データ W_{i+1} と、及び今回受信した次々回認証データの正当性検証データ M_{i+1} とを、上記登録データ記憶手段に登録されているデータ W_{i+1} 、

W_{i+1} 、 M_{i+1} と置き換えて登録し、認証回数 n をインクリメントする。

【請求項 20】 ネットワーク上で認証者からユーザに対する認証を得るユーザ側の手順を記録した記録媒体であり、上記手順は、以下を含む：

(a) サービス要求とユーザの識別子 A を上記認証者装置に送信し、

(b) n を正の整数とすると、上記認証者装置から認証回数 n を受信し、

(c) (+) を排他的論理和とすると、上記ユーザの識別子 A 、受信した上記認証回数 n 及び秘密に保持しているパスワード S を用いて、今回の被認証データ V_{i+1} 、次々回の認証データ W_{i+1} 、上記次々回認証データ W_{i+1} の正当性検証データ M_{i+1} を次の一方向性関数

$$V_{i+1} = E(A, S(+)(n-1))$$

$$V_i = E(A, S(+)(n))$$

$$V_{i+1} = E(A, S(+)(n+1))$$

$$W_{i+1} = E(A, V_{i+1})$$

$$M_{i+1} = E(W_{i+1}, V_{i+1})$$

により算出し、上記認証者装置に送信する。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、特に、インターネットのように容易に盗聴され易い、つまり安全性（セキュリティ）が十分でないネットワークにおいて、高速で小規模のプログラムでパスワードを用いたユーザ認証を行い、安全に情報の送受信を実現することのできる情報送受信制御方法（プロトコル）に関するものである。

【0002】

【従来の技術】 インターネットの普及に伴い、通信の際に、通信相手やユーザの資格を認証することが不可欠に

なっている。認証方法には様々な技術が存在するが、大きく分けて、公開鍵暗号方法を応用したものと共通鍵暗号方法を応用したものの二つに分類することができる。

【0003】このうち、公開鍵暗号方法を用いる方法は、その性質上、優れた認証能力を有しており、電子取引などへの応用が期待されている。しかし、処理に時間がかかり、また、プログラムサイズが大きいため、PDA (Personal Digital Assistant: 携帯端末) 等の処理能力の低い端末やインターネット関連の通信プロトコルなどへの組み込みにおいては、その適用領域が制限されるという問題がある。

【0004】そこで、このような適用域には、公開鍵暗号方法より格段の高速処理が可能な共通鍵系の暗号方法を応用した方法、特に、パスワード認証方法がよく用いられる。基本的なパスワード認証の手順は以下の通りである。まず、被認証者が認証者にパスワードを登録する。認証時に、被認証者が認証者にパスワードを送信する。認証者は、受信したパスワードと登録されているパスワードを比較する。

【0005】この方法には、次のような問題点がある。
(a) 認証側にあるパスワードファイルの盗見により、パスワードが盗まれる。
(b) 通信中、回線盗聴によってパスワードが盗まれる。
(c) 被認証者は認証者に、自分の秘密情報であるパスワードを公開する必要がある。

【0006】最初の問題(a)を解決する方法として、被認証者が認証者側に、パスワードに一方方向性関数を施したデータを登録しておき、認証時に、認証者が受信したパスワードに同じ一方方向性関数を施し、結果を比較するという方法(参考文献: A. Evans, W. Kantrowitz and E. Weiss: "A user authentication scheme not requiring secrecy in the computer," Commun. ACM, 17, 8, pp. 437-442(1974)及びR. Morris and K. Thompson: "Password security: A case history," UNIX Programmer's Manual, Seventh Edition, 2B(1979))がある。

【0007】一方方向性関数とは、入力の総当たり以外に、出力から入力を得る効率的な手段が存在しない関数であり、総当たりの計算量を充分大きくしておけば、無資格者が入力データを算出して被認証者になりすますことを防ぐことができる。一般に、一方方向性関数は、DESやFEALなどの共通鍵暗号方法によって得ることができる。共通鍵暗号方法は、共通秘密鍵を用いて入力される平文を処理して暗号文を出力として得るもので、平文と暗号文が与えられても共通秘密鍵が算出できない。即ち、共通秘密鍵は鍵の総当たりより効率的に得る手段がないように設計されている。したがって、この手法により平文と任意のパラメータ、共通秘密鍵を入力、暗号文を出力とすることによって、共通鍵暗号方法の強さに依存した一方方向性関数を実現することができる。更に、

DES, FEALなどの共通鍵暗号方法は、平文や共通秘密鍵の入力が1ビット変化しただけでも、その入力変化の痕跡をまったくとめない出力を得ることができるという特徴を有している。

【0008】以上説明した通り、一方方向性関数を用いた方法によって、基本的なパスワード認証方法の最初に指摘した問題は解決できる。しかし、これを回線盗聴が簡単なインターネットに適用する場合、問題(b)を解決することはできない。また、問題(c)で指摘したように、この基本的なパスワード認証方法は、銀行の顧客認証などには適用できても、同一レベルのユーザ同士の認証には適していない。

【0009】このような問題を解決する方法として、Lamportの方法(L. Lamport: "Password authentication with insecure communication," Commun. ACM, 24, 11, pp. 770-772(1981)), 及びこの出願の発明者が提案した動的パスワード認証方法であるCINON法(Chained One-way Data Verification Method) (A. Shimizu, "A Dynamic Password Authentication Method Using a One-way Function" Systems and Computers in Japan, Vol. 22, No. 7, 1991, pp. 32-40)がある。

【0010】Lamportの方法は、パスワードに一方方向性関数を複数回適用しておいて、適用一回前のデータを次々と認証者側に示すことで、複数回の認証を可能にする方法である。この方法では、最初に設定した最大認証回数から認証を実行する毎に1を減算し、認証回数を使い尽くした時点で、パスワードを再設定する必要がある。最大認証回数を増やすために一方方向性関数の適用回数を増加させると処理量が增大する。更に、認証者側に比較して処理能力の小さい、被認証者側の処理負担が大きいという問題点がある。

【0011】これらの問題点を解決する方法 CINONは、被認証者(ユーザ)が認証者(ホスト)に対して、前回に正当性の検証を終え登録されている被認証データのものとのデータ、次々回に認証に用いる被認証データ、前回送信済みで次の認証に用いる被認証データの正当性検証データの3つのデータを認証毎に送信することで、認証情報を安全に更新しながら次々と連鎖的に認証を行うことのできる方法である。

【0012】以下に、CINONの認証手順を説明する。まず、以降の説明に用いる記法を示す。

<記法>共通鍵暗号アルゴリズムEによる一方方向性変換を $C=E(P, K)$ で表す。Cは一方方向性変換データ、Pは平文、Kは共通鍵である。

【0013】Sを、被認証者の秘密情報、即ち、パスワードとする。nは0以上の整数であり、認証回数を示す。Aを被認証者の識別子、即ち、例えばメールアドレス(被認証者への情報が蓄積される部分)などのユーザIDとする。Nを、認証回数nに対応して発生する乱数とする。

【0014】 M_i を認証子とする。 $(+)$ はビット毎の排他的論理和を表す。 $V_i = E(A, S(+)N_i)$ とするとき、 $W_i = E(A, V_i)$ とする。即ち、 W_i は、 $S(+)N_i$ に2度一方向性変換を施したデータであり、 W_i から、 S 、 N_i あるいは V_i を逆算することの困難さは、共通鍵暗号アルゴリズムの強さに依存している。

【0015】＜CINONの認証手順（図1参照）＞

--初期登録処理--

ステップS0：被認証者（ユーザ）は初期登録処理を認証者の装置（ホスト装置）で行う。まず、 $n=0$ とし、ユーザはユーザ端末で乱数 N_0 、 N_1 を生成し、被認証者識別子AとパスワードSを設定する。ユーザはパスワードSを覚えておき、乱数 N_0 、 N_1 を自分のICカード等の媒体に保存しておく。

【0016】次に、以下の手順：

$$V_0 = E(A, S(+)N_0)$$

$$W_0 = E(A, V_0)$$

$$V_1 = E(A, S(+)N_1)$$

$$W_1 = E(A, V_1)$$

$$M_0 = E(W_0, V_0)$$

$$n \leftarrow n + 1$$

で W_0 、 W_1 、 M_0 を算出し、ユーザ識別子Aと対応させて認証回数 n と共に認証側装置（ホスト装置）に登録しておく。 W_i は次回の認証データ、 W_i は次々回の認証データ、 M_i は W_i の正当性検証データである。

--認証処理およびコンテンツデータのやりとり--

初期登録処理（ $n=0$ ）終了後、第 n 回目（ $n=1, 2, \dots$ ）の認証処理は以下の通りである。なお、この時点で、認証者側には、被認証者の識別子Aに対応して $W_{0..i}$ 、 W_i 、 $M_{0..i}$ 、 n が登録されている。被認証者からのサービス起動要求を受信すると、登録してある n を返信する。

【0017】ステップS1：ユーザは、まず、認証者に対してユーザ識別子Aとサービス要求を送り、サービス起動要求を行う。

ステップS2：次に、ホスト装置はユーザ識別子Aに対応して登録されている n の値をユーザに送る。

ステップS3：ユーザは認証者より n の値を受け取り、ICカードから乱数 $N_{0..i}$ 、 N_i を読みだし、新しく乱数 N_{i+1} を発生させ、以下の手順：

$$V_{i+1} = E(A, S(+)N_{i+1})$$

$$V_i = E(A, S(+)N_i)$$

$$V_{0..i} = E(A, S(+)N_{0..i})$$

$$W_{i+1} = E(A, V_{i+1})$$

$$M_i = E(W_{0..i}, V_i)$$

で V_{i+1} 、 W_{i+1} 、 M_i を算出する。

【0018】ステップS5：ユーザはこれらのデータを認証者に送付する。 V_{i+1} は、認証者側において、前回に正当性の確認を終え、今回の認証に用いるデータ W_{i+1} のもととなったと推定されるデータである。 W_{i+1} は、次々回の認証に用いるデータである。また、 M_i は、次々回

の認証に用いるデータ W_{i+1} の正当性検証を次回に検証するためのデータである。

【0019】ステップS6：また、ユーザはICカードの乱数 $N_{0..i}$ 、 N_i を N_{i+1} 、 N_{i+1} に書き換える。

ステップS7：次に、ホスト装置は被認証者側より送付されてくる V_{i+1} 、 W_{i+1} 、 M_i により、以下の認証処理を行う。

W_{i+1} と $E(A, V_{i+1})$ を比較し、一致した場合、被認証者を正当とする。一致しない場合、その被認証者を不当とし、処理を終了する。

【0020】被認証者を正当とした場合、更に、 M_{i+1} と $E(W_{0..i}, V_i)$ を比較し、一致した場合、 W_{i+1} を正当とする。一致しない場合、ユーザを不当とし処理を終了する。この2つの検証で共に被認証者を正当とした場合、 W_{i+1} 、 W_i 、 M_{i+1} は全て正当であると認証し、ステップS8でコンテンツデータTをユーザに送付する。また、ステップS9で現在登録してあるデータに換えて、 W_{i+1} 、 W_i 、 M_i を新たに登録する。また、 n をインクリメント（+1）する。

20 【0021】このように、CINON では、ユーザが認証者の認証を得るためには、前回生成した2つの乱数 $N_{0..i}$ 、 N_i を使用する必要がある。そのため、ユーザが出先の端末から認証者の認証を得る場合には、ユーザはそれらの乱数 $N_{0..i}$ 、 N_i を記憶した例えばICカードの様な記憶媒体を携帯し、出先の端末で使用しなければならない。また、端末は、乱数を発生する機能及びICカードを読み書きする機能を必要とする。一方、インターネットにおいては、テレビセットやワードプロセッサ、更に携帯端末などにインターネット接続機能を付加したインターネット家電と呼ばれる製品が市場投入されようとしている（参考文献：荒川、鎌田：“インターネット家電がもたらす情報ネットワーク革命、” 信学技報、OFS96-1, pp.1-6(1996.5)）。

【0022】このようなインターネット家電が普及してくることに伴い、認証処理を有した情報の送受信に対する需要が増大してくるものと思われるが、インターネット家電は、コストを最重視しているため、上述の乱数 $N_{0..i}$ 、 N_i を発生したり、それらをICカード等の記憶媒体へ読み書きする機構を有していない場合がほとんどである。また、処理プログラムの格納領域も限られるため、このような認証処理をできるだけ簡易で小さいプログラムサイズで実現することが望まれる。

【0023】

【発明が解決しようとする課題】この発明の目的は、セキュリティが十分でないネットワーク上の被認証者と認証者間の情報送受信において、被認証者側にICカード等の記憶媒体の読み書きを行う機構を必要とせず、かつユーザ認証処理を小さいプログラムサイズで行うことができる安全な情報送受信制御方法と装置、及びその方法を記録した記録媒体を提供することにある。

【 0024】

【課題を解決するための手段】この発明の第1の観点によれば、ネットワーク上でユーザが利用するユーザ端末装置と、認証者の認証者装置との間で認証処理を行うための情報送受信制御方法であり以下のステップを含む：

(a) 初期登録手順として、上記ユーザが、自分の識別子Aと、秘密に保持しているパスワードSから、次回認証データ W_1 、次々回認証データ W_2 、次々回認証データ W_3 の正当性検証データ M_1 の3つを算出し、認証回数nの初期値 $n=1$ と共に上記認証者装置に上記識別子Aと対応して登録し、(b) 次に、nを正の整数とすると、第n回目の認証において、上記認証者装置は、上記ユーザ端末装置からサービス起動要求と上記ユーザの識別子Aの通知を受けて、そのユーザの認証回数nを読みだし、そのユーザ端末装置へ通知し、(c) 上記ユーザ端末装置では、上記ユーザの識別子A、送られてきた上記認証回数n及び秘密に保持しているパスワードSを用いて、今回の認証されるべきデータ V_{n-1} 、次々回の認証に用いられるデータ W_{n-1} 、その次々回認証データ W_{n+1} の正当性を検証するためのデータ M_n を算出し、送信したいコンテンツデータがある場合には、そのデータと共に上記認証者装置に通知し、(d) 上記認証者装置では、上記ユーザの識別子Aと上記ステップ(c)で送付されてきた今回の認証されるべきデータ V_{n-1} とから算出したデータ W_{n-1} を、登録されている認証データ W_{n-1} と比較し、かつ登録されている次回認証データ W_n と、上記今回の被認証データ V_{n-1} とから計算した正当性検証データ M_{n-1} を、登録されている正当性検証データ M_{n-1} と比較し、(e) 上記ステップ(d)の比較の結果、一致した場合、上記認証者装置では、そのユーザを正当とし、上記ユーザが要求したサービスの情報の送受信を行うとともに、前回受けた次回認証データ W_n と、今回送付されてきた次々回認証データ W_{n+1} と、次々回認証データ W_{n+1} の正当性検証データ M_n を、前回登録した W_{n-1} 、 W_n 、 M_{n-1} と置き換えて登録し、認証回数nをインクリメントし、(f) 上記ステップ(d)の比較の結果、一致しない場合、そのユーザを不当とし以降の情報送受信を拒否し、前回登録した W_{n-1} 、 W_n 、 M_{n-1} 及びnをそのまま保持する。

【 0025】この発明の第2の観点によれば、インターネットにユーザ端末装置と中継サーバがそれぞれ接続されており、そのインターネットに接続されたイントラネットに認証者装置が接続されており、上記ユーザ端末装置と上記認証者装置との間の情報送受信を、上記中継サーバを介して行うシステムにおいて、上記ユーザと認証者との間で認証処理を行うための情報送受信制御方法であり、以下のステップを含む：

(a) 上記ユーザの識別子Aと、秘密に保持しているパスワードSから、次回認証データ W_1 、次々回認証データ W_2 、その次々回認証データ W_3 の正当性検証データ M_1 の3つを算出し、上記認証者装置に上記識別子Aと対応して

登録し、上記認証回数nの初期値 $n=1$ を上記認証者装置と上記中継サーバにそれぞれ上記識別子Aと対応させて保持し、(b) nを正の整数とすると、第n回目の認証において、上記中継サーバは上記ユーザ端末装置からサービス要求と識別子Aを受けると、対応する認証回数nを読みだし、上記ユーザ端末装置に送り、(c) 上記ユーザ端末装置では、上記ユーザの識別子A、送られてきた上記認証回数n及び秘密に保持しているパスワードSを用いて、今回の認証されるべきデータ V_{n-1} 、次々回の認証データ W_{n-1} 、その次々回認証データ W_{n+1} の正当性検証データ M_n を算出し、送信したいコンテンツデータがある場合には、そのデータと共に上記中継サーバを介して上記認証者装置に送り、その後上記中継サーバとの接続を一旦切断し、(d) 上記認証者装置では、上記ユーザの識別子Aと上記ステップ(c)で送付されてきた今回の被認証データ V_{n-1} とから算出した今回の認証データ W_{n-1} を、登録されている認証データ W_{n-1} と比較し、かつ登録されている次回認証データ W_n と、上記今回の被認証データ V_{n-1} とから計算した正当性検証データ M_{n-1} を、登録されている正当性検証データ M_{n-1} と比較し、(e) 上記ステップ(d)の比較の結果、一致した場合、上記認証者装置では、そのユーザを正当とし、上記ユーザが要求したサービスの情報を上記中継サーバに転送して、そこに保管し、或いは、送信したいコンテンツ情報がある場合には、認証されたユーザの資格でその情報の送信を行い、送信を完了したことを示す確認情報を中継サーバに送信し、(f) 上記認証者装置は更に、前回受けた次回認証データ W_n と、今回送付されてきた次々回認証データ W_{n+1} と、その次々回認証データの正当性検証データ M_n を、前回登録した W_{n-1} 、 W_n 、 M_{n-1} と置き換えて登録し、認証回数nをインクリメントし、上記ステップ(d)の比較の結果、一致しない場合、そのユーザを不当とし以降の情報送受信を拒否し、前回登録した W_{n-1} 、 W_n 、 M_{n-1} 及びnをそのまま保持し、(g) 上記中継サーバは、上記サービス情報或いは上記送信確認情報を受け取った後、上記認証回数nをインクリメントし、(h) 上記ユーザは、上記中継サーバとの接続を切断してから一定時間が経過した後の任意の時間に上記中継サーバに再度接続し、上記中継サーバとの間で上記サービス情報に対する上記ユーザの正当性を検証する認証処理を行い、上記サービス情報を受信し、ここで、上記ユーザ端末装置と上記中継サーバ間の情報のやりとりは高速通信プロトコルを使って行い、上記中継サーバと上記認証者装置間の情報のやりとりは電子メールプロトコルを使って行う。

【 0026】この発明の第3の観点によれば、ユーザ端末装置と、サービスプロバイダと、認証者装置（課金管理センタ）とがインターネットに接続されており、ユーザがインターネット上でサービスプロバイダからサービスを受ける場合に、ユーザが課金管理センタとの間で認証処理を行うための情報送受信制御方法であり、以下のステ

ップを含む：

(a) 初期登録手順として、上記ユーザのアカウント A と、パスワード S から次回認証データ W_1 、次々回認証データ W_2 、その次々回認証データの正当性検証データ M_1 の 3 つを計算し、認証回数初期値 $n=1$ と、金額 X と共に上記アカウント A と対応して登録し、(b) ユーザは上記サービスプロバイダに所望のサービスを要求するサービス要求信号とアカウント A を送り、(c) 上記サービスプロバイダは受信した上記アカウント A を上記課金管理センタに転送し、(d) 上記課金管理センタは上記アカウント A に対応する認証回数 n を読み出し、上記サービスプロバイダに送り、(e) 上記サービスプロバイダは受信した認証回数 n を認証手順の Applet プログラムと共にユーザ端末装置に送り、(f) 上記ユーザは上記認証手順に従って認証用データ V_{n-1} 、 W_{n-1} 、 M_{n-1} を計算し、上記アカウント A と共に上記サービスプロバイダに送り、(g) 上記サービスプロバイダはデータ V_{n-1} 、 W_{n-1} 、 M_{n-1} と共に上記サービスプロバイダのアカウント A_r と、上記サービスに対する金額 x を上記課金管理センタに送り、(h) 上記課金管理センタは上記サービス金額 x が上記アカウント A に対応して登録されている残額 X 以下であることを確認し、受信したデータ V_{n-1} と登録されている次回認証データ W_n を検証し、両方とも正しければ認証確認信号 OK を上記サービスプロバイダに送ると共に、データ W_n 、 W_{n+1} 、 M_n に更新し、認証回数 n をインクリメントし、上記アカウント A の残額 X を $X-x$ で更新し、上記プロバイダのアカウント A_r の残額 XP を X_r+x で更新し、(i) 上記サービスプロバイダは、上記確認信号 OK を受けると上記ユーザに上記指定されたサービスを提供する。

【0027】この発明の第4の観点によれば、ネットワーク上でユーザの正当性を認証するための情報送受信制御を行う認証者装置であり、以下を含む： n を正の整数とすると、次回認証データ W_{n-1} 、次々回認証データ W_n 、次々回認証データ W_n の正当性検証データ M_{n-1} を認証回数 n と共に上記識別子 A と対応して第 $n-1$ 回目の認証時に登録した登録データ記憶手段と、第 n 回目の認証において、上記ユーザの端末装置からサービス起動要求と上記ユーザの識別子 A の通知を受けて、そのユーザの認証回数 n を上記登録データ記憶手段から読みだし、そのユーザ端末装置へ通知する認証回数送出手段と、上記ユーザ端末装置から送られてきた今回の被認証データ V_{n-1} 、次々回の認証データ W_{n-1} 、次々回認証データ W_n の正当性検証データ M_{n-1} を受信する受信手段と、上記ユーザの識別子 A と上記受信した今回の被認証データ V_{n-1} とから算出した今回の認証データ W_n を、上記登録データ記憶手段に登録されている認証データ W_{n-1} と比較し、かつ登録されている次回認証データ W_n と、上記今回の被認証データ V_{n-1} とから計算した正当性検証データ M_{n-1} を、登録されている正当性検証データ M_{n-1} と比較する認証手段と、及び上記認証手段による比較の結果、一致した場合、その

ユーザを正当とし、登録されている次回認証データ W_n と、今回受信した次々回認証データ W_{n+1} と、及び今回受信した次々回認証データ W_{n+1} の正当性検証データ M_n とを、上記登録データ記憶手段に登録されている W_{n-1} 、 W_n 、 M_{n-1} と置き換えて登録し、認証回数 n をインクリメントする登録更新手段。

【0028】この発明の第5の観点によれば、ネットワーク上でユーザの正当性を認証する認証者側の認証手順を記録した記録媒体であり、上記認証手順は以下を含む：

(a) ユーザの識別子 A とパスワード S を使って次の一方方向性関数

$$V_0 = E(A, S)$$

$$W_0 = E(A, V_0)$$

$$V_1 = E(A, S(+1))$$

$$W_1 = E(A, V_1)$$

$$M_0 = E(W_1, V_0)$$

によりデータ初期値 W_0 、 W_1 、 M_0 を算出して登録し、(b) n を正の整数とすると、第 n 回目の認証において、上記ユーザの端末装置からサービス起動要求と上記ユーザの識別子 A の通知を受けて、そのユーザの認証回数 n を上記登録データ記憶手段から読みだし、そのユーザ端末装置へ送信し、(c) 上記ユーザ端末装置から送られてきた今回の被認証データ V_{n-1} 、次々回の認証データ W_{n-1} 、次々回認証データ W_n の正当性検証データ M_{n-1} を受信し、

(d) 上記ユーザの識別子 A と上記受信した今回の被認証データ V_{n-1} とから一方方向性関数 $W_{n-1} = E(A, V_{n-1})$ により今回の認証データ W_n を算出し、上記登録データ記憶手段に登録されている認証データ W_{n-1} と比較し、かつ登録されている次回認証データ W_n と、上記今回の被認証データ V_{n-1} とから一方方向性関数 $M_{n-1} = E(W_n, V_{n-1})$ により正当性検証データ M_{n-1} を算出し、登録されている正当性検証データ M_{n-1} と比較し、(e) 2 つの比較結果が同時に一致であった場合、そのユーザを正当とし、登録されている次回認証データ W_n と、今回受信した次々回認証データ W_{n+1} と、及び今回受信した次々回認証データの正当性検証データ M_n とを、上記登録データ記憶手段に登録されている W_{n-1} 、 W_n 、 M_{n-1} と置き換えて登録し、認証回数 n をインクリメントする。

【0029】この発明の第6の観点によれば、ネットワーク上で認証者からユーザに対する認証を得るユーザ側の手順を記録した記録媒体であり、上記手順は以下を含む：

(a) サービス要求とユーザの識別子 A を上記認証者装置に送信し、(b) n を正の整数とすると、上記認証者装置から認証回数 n を受信し、(c) 上記ユーザの識別子 A、受信した上記認証回数 n 及び秘密に保持しているパスワード S を用いて、今回の被認証データ V_{n-1} 、次々回の認証データ W_{n-1} 、次々回認証データ W_n の正当性検証データ M_{n-1} を次の一方方向性関数

$$V_{n+1} = E(A, S(+)(n-1))$$

$$V_n = E(A, S(+)(n))$$

$$V_{n+1} = E(A, S(+)(n+1))$$

$$W_{n+1} = E(A, V_{n+1})$$

$$M_n = E(W_{n+1}, V_n)$$

により算出し、上記認証者装置に送信する。

【0030】この発明は、認証手順において、従来技術において被認証データ生成時に用いていた乱数に代えて、認証回数を用いるようにしたことを最も主要な特徴とする。この発明においては、被認証データの生成に用いる一方向性変換にDESやFEALなどの共通鍵暗号方法を用いる。これらの暗号方法は、先述の通り、平文や共通秘密鍵の入力が1ビット変化しただけでも、その入力の痕跡をまったくとどめない出力を得ることができる。一方向性変換のこの特徴に着目し、従来技術が、乱数と秘密に保持しているパスワードの2つを鍵にして被認証データを生成していたのに対して、一方を定数である認証回数とすることで、従来と同等の強度を持つ認証機能を有し、かつ、この発明の目的である乱数を記憶するためのICカード及びそれに対する読み書き機構、乱数発生機構を必要としない簡易な情報送受信を実現することができる。つまりこの発明では従来の乱数にかえ認証回数を用いているが、安全性は用いる一方向性関数、つまり共通暗号方法の強度に依存し、認証回数に変更した影響はない。

【0031】

【発明の実施の形態】

実施例1

図2は、この発明の第1の実施例の概要を説明する図である。インターネットの普及により、電子メールがインターネットを介したコミュニケーションの手段として、特にビジネスの分野において幅広く用いられるようになってきた。これに伴い、ビジネスユーザを中心に、出先からメールメッセージを送受したいといった要求が高まってきている。

【0032】パソコン通信の場合は、電話網を用いて共通のセンタへアクセスし、メッセージの読み出しや書き込みを行うため、例えば出先端末からでも、ISDN公衆電話網にモデム機能を有した携帯型のパソコンを接続するなどして、メッセージの送受信を行うことができる。これに対して、インターネットでは、電話網におけるパソコン通信と同じように、メールサーバをセンタと考えて電話網経由でアクセスすることが可能であるが、セキュリティ上の問題から、あらかじめ登録してある電話番号にコールバックさせたり、モデム経由でのアクセスを制限している場合が多い。また、一般にモデムアクセス用に用意している電話回線の数はいくつか、回線が話中でつながらない場合が多いなど、場所が定まらない出先からのアクセスは困難である場合が多い。

【0033】また、インターネット本来の特徴であるIP

アドレスレベルでの接続（レイヤ3での接続）を考えた場合、不定な出先、即ち、不特定のIPアドレスからの接続要求は、メールサーバ13のある内部ネットワーク12への入口に設けてあるファイアウォール12Fによって拒否される。つまり、電子メール（レイヤ7）で使われるプロトコル（即ちSMTP: Simple Mail Transfer Protocol）はファイアウォールを通過することができるように決められている。この実施例では、出先から電話網を使わず、ファイアウォールを回避して、インターネット経由で安全に自分宛のメールメッセージを取り出したり送信したりすることのできる公衆電子メール転送サービスにおけるメールサーバの、ユーザに対する認証にこの発明を適用した場合を説明する。

【0034】公衆電子メール転送サービスが有するべき一般要求およびセキュリティ上の要件について述べる。まず、この明細書で扱う公衆電子メール転送サービスが有する一般要件は以下の通りである。

(1) このサービスのユーザ（利用者）は、インターネット上のあるメールサーバに固有のメールアカウントを有している。

【0035】(2) ユーザは、ユーザ固有のメールアカウントがある環境において常駐されたこのサービスのアプリケーションを、また、出先の環境において、このサービスのアプリケーションプログラムを用いることができる。

(3) ユーザは、出先において、テンポラリなアカウントを用い、本来のアカウント宛に届いている電子メールを受信できる。同様に、テンポラリなアカウントを用い、本来のアカウントからのメール送信ができる。ここで、テンポラリなアカウントとは、例えば公衆に使用が提供されている、インターネットに接続された端末や、他ユーザのアカウントなどである。

【0036】図2の例ではインターネット11に企業内のLANのような内部ネットワーク12が接続され、その内部ネットワーク12に、ユーザU1のメールアカウントがあるホスト装置（サーバ装置：認証者装置）13が接続され、ユーザU1はホスト装置13の接続された内部ネットワーク12を通じて、ホスト装置13の自己のメールアカウント宛に届いている電子メールを受信できる。

【0037】ユーザU1が移動して、内部ネットワーク12の外部へ移動した状態で、その移動先の、インターネット11に加入している例えばパソコン14にユーザU1の識別子AとパスワードSを入力し、ユーザU1の識別子Aを電子メールとしてインターネット11、内部ネットワーク12を介して、ユーザU1のメールアカウントがあるホスト装置（被認証者装置）13へ送り、ホスト装置13との間でこの発明による認証手順を実施すれば、ユーザU1のメールアカウント宛に届いている電子メールを受信することができる。つまりパソコン14が

インタネット 11 に加入しているアカウントを一時的に借りて、本来のアカウント A に宛ている電子メールを受信できる。

【0038】更にインタネット 11 と接続された他の内部ネットワーク 15 に収容されている端末 16 にユーザ U1 は自己の識別子 A、パスワード S を入力し、識別子 A を電子メールとして内部ネットワーク 15 - インタネット 11 - 内部ネットワーク 12 を介してホスト装置 13 に入力して、この発明による認証手順を実施することにより、その自己メールアドレスに届いている電子メール

【0039】しかし、別のユーザ U2 が端末 17 を通じて、ユーザ U1 になりすまして、そのメールアドレスに届いている情報を取出そうとしても、即ち、ユーザ U1 の識別子 A を使ってホスト装置 13 にアクセスしたとしても、ユーザ U1 のパスワード S を知らないため、認証手順を正しく実行できず、ホスト装置 13 のユーザ U1 のメールアドレスに届いた情報を取出すことはできない。

【0040】上述では電子メールの読出し（受信）について述べたが、電子メールの書込み（送信）も同様に行うことができる。公衆電子メール転送サービスが有するべき一般的要件により、以上のように電子メールの受信、送信が可能であるが、この公衆電子メール転送サービスが有するべきセキュリティ上の要件は以下の通りである。

【0041】(1) ユーザは、記憶しているパスワード等が認証されることによって、メールサーバのある環境に設定されたファイアウォールを回避でき、出先において、安全にメール送受信サービスの提供を受けることができる。これに対して、資格のない者のメール送受信は阻止される。

(2) 回線およびメールサーバ内データベースから、ユーザのパスワードを盗取できない。

【0042】(3) 認証のための処理負担が、ユーザのメールアドレスがある環境および出先の環境の双方において少ない。特に、インタネット上を流れるデータは、簡単に盗聴されるため、パスワードが回線上をそのまま流れるような手順は用いられない。第 1 実施例はこのような条件 (1)、(2)、(3) を満たす電子メール転送サービスにおける認証手順にこの発明を適用した場合である。従って、ユーザとメールサーバ間の通信は電子メールのプロトコルを使って行う。なお、以下の説明に用いる記法は、従来技術の説明に用いたものと同じである。

<初期登録処理 (図 3)> ステップ S0 : 初期登録処理として、ユーザは識別子 (メールアドレス) A と認証回数初期値 $n=0$ をメールサーバ 13 に直接設定する。

【0043】次に、ユーザはメールサーバ 13 において以下の手順：

$$V_0 = E(A, S) \quad (1a)$$

$$W_0 = E(A, V_0) \quad (1b)$$

$$V_1 = E(A, S(+1)) \quad (1c)$$

$$W_1 = E(A, V_1) \quad (1d)$$

$$M_0 = E(W_1, V_0) \quad (1e)$$

で W_0 、 W_1 、 M_0 を算出し、ユーザのメールアドレス A に対応させてメールサーバ (認証者装置) 内に登録しておく。更に、 n を 1 にインクリメントし、識別子 A に対応して登録しておく。 W_0 は次回の認証データ、 W_1 は次々回の認証データ、 M_0 は W_1 の正当性検証データをそれぞれ表している。

<認証処理およびメールメッセージのやりとり> 図 3 は初期登録処理終了後、第 n 回目 ($n=1, 2, \dots$) の認証手順を以下に示す。

【0044】ステップ S1 : 出先にいるユーザは、出先の端末 (図 2 における端末 14) を使ってまず自分のメールアドレスがあるメールサーバに対して、特定のヘッダ (SMTP) を有する電子メールでメールサービス要求 (以下、メール要求と呼ぶ) を送出すると共にメールアドレス A を通知する。メール要求は、メール送信、メール受信、ファイル転送送信、ファイル転送受信のいずれかを指定するものである。

【0045】ステップ S2 : メールサーバは出先にいるユーザからのサービス起動要求メールを受信すると、メールアドレス A に対応して登録してある認証回数 n を、メールで返信する。この時点で、ホスト側には、既に、 W_{n-1} 、 W_n 、 M_{n-1} が登録されている。

ステップ S3 : ユーザはメールサーバからメールで、 n の値を受け取り、以下の手順：

$$V_{n-1} = E(A, S(+)(n-1)) \quad (2a)$$

$$V_n = E(A, S(+)(n)) \quad (2b)$$

$$V_{n+1} = E(A, S(+)(n+1)) \quad (2c)$$

$$W_{n-1} = E(A, V_{n-1}) \quad (2d)$$

$$M_n = E(W_{n-1}, V_n) \quad (2e)$$

で V_{n-1} 、 W_{n-1} 、 M_n を算出し、更に、ステップ S4 でメールにより、これらのデータ、および送信したいメールのある場合にはその情報を、自分のメールサーバに送付する。 V_{n-1} はメールサーバ側において、前回に正当性の確認を終え、今回の認証に用いる、一方向性関数の変換により得られるデータ (一方向変換データと呼ぶ) W_{n-1} の元となったと推定されるデータである。 W_{n-1} は、次々回の認証に用いる一方向変換データである。また、 M_n は次々回の認証に用いる一方向変換データ W_{n-1} の正当性を次回に確認するための認証データである。

【0046】ステップ S5 : メールサーバは、ユーザ側より受信した V_{n-1} 、 W_{n-1} 、 M_n により、以下の認証処理を行う。登録されている W_{n-1} と、受信した V_{n-1} を使って一方向性関数 E により計算した $E(A, V_{n-1})$ とを比較し、一致した場合、ユーザを正当とする。一致しない場合、そのユーザを不当とし、処理を終了する。

【0047】ユーザを正当とした場合、更に、 W_{n-1} と E

(W_n, V_{n+1})を比較し、一致した場合、 W_n を正当とする。一致しない場合、 W_n を不当とし処理を終了する。正当とされたこの W_n は次回($n+1$)の認証においてデータ W_{n+1} として受信 V_{n+1} の正当性(ユーザの正当性)の判定に使用されることになる。これらの認証処理によりユーザ及び W_n が正当と判定された場合、ステップS6でユーザ宛の到着メールがあれば、それをユーザにメールで送付する。また、ユーザからの送信メールがある場合には、ユーザの本来のアカウントでそのメールを送信する。

【0048】更に、ステップS7で現在登録してあるデータ W_{n+1}, W_n, M_{n+1} に換えて、 W_n, W_{n+1}, M_n を新たに登録する。また、 n をインクリメントする。図4は上述の第1実施例で使用されるユーザ端末の機能ブロック図を示す。ユーザ端末は、入力部21と、制御部22と、受信部23と、送信部24と、認証用データ生成部30と、メモリ25と、出力部26とから構成されている。入力部21にはユーザが識別子A、パスワードS、接続先アドレス(メールサーバアドレス)、メール要求、等の情報を入力する。制御部22はメールサーバにメール要求及び識別子Aを送信部24から送信すると共に、認証用データ生成部30に識別子AとパスワードSを設定する。受信部23により受信されたメールサーバからの認証回数 n は減算部31aで1が減算され、その出力 $n-1$ が排他的論理和部32aでパスワードSと排他的論理和が取られる。排他的論理和部32aの出力は識別子Aと共に一方向性関数部33aに与えられ、式(2a)によりデータ V_{n+1} が計算される。受信部23からの認証回数 n は加算部31cにも与えられ、1が加算され、その加算結果 $n+1$ が排他的論理和部32cでパスワードSと排他的論理和が取られる。排他的論理和部32cの出力は識別子Aと共に一方向性関数部33cに与えられ、式(2c)によりデータ V_{n+1} が計算される。データ V_{n+1} は識別子Aと共に更に一方向性関数部34dに与えられ、式(2d)によりデータ W_{n+1} が計算される。認証回数 n は更に排他的論理和部32bにも与えられ、パスワードSとの排他的論理和が取られる。その出力は識別子Aと共に一方向性関数部33bに与えられ、式(2b)によりデータ V_n が計算され、更に、データ V_n と一方向性関数部34dの出力 W_{n+1} が一方向性関数部34eに与えられ、式(2e)によりデータ M_n が計算される。この様にして計算された認証用データ V_{n+1}, W_{n+1}, M_n はレジスタ35に一時的に保持され、送信部24からメールサーバに送出される。

【0049】メールサーバ13による認証後、メールサーバ13から受信したメールメッセージはメモリ25に一時保持され、必要に応じてプリンタ或いは表示器などの出力部26に出力する。図4に示したユーザ端末の機能構成における制御部22、メモリ25、認証用データ生成部30は実際にはコンピュータのソフトウェアとして実現される。即ち、端末コンピュータは図3における

ユーザ側処理手順を実行するプログラムが記録された記録媒体を有しており、そのプログラムに従ってユーザ側の認証処理手順を実行する。

【0050】図5は、図2及び3の実施例におけるメールサーバ13の機能ブロック図を示す。メールサーバ13は入力部41、初期登録部50、認証部60、制御部44、認証回数歩進部45、メモリ43から構成されている。初期登録部50は、初期登録時(ステップS0)にユーザにより入力部41から入力された識別子(メールアドレス)AとパスワードSとから式(1a)により V_n を計算する一方向性関数部51と、その V_n と識別子Aから式(1b)により W_n を計算する一方向性関数部52と、式(1c)中のパスワードSと1との排他的論理和を計算する排他的論理和部53と、その排他的論理和出力と識別子Aとから式(1c)により V_n を計算する一方向性関数部54と、 V_n とAとから式(1d)により W_n を計算する一方向性関数部55と、 W_n と V_n とから式(1e)により M_0 を計算する一方向性関数部56とから構成されている。

【0051】制御部44はこれらの計算した初期値 W_n, W_n, M_n を識別子Aと対応させてメモリ43に登録する。また、歩進部45により認証回数 n を1インクリメントして識別子Aに対応させてメモリ43に記憶する。ユーザの n 回目の認証において、レジスタ46には、メモリ43から読み出した認証回数 n を歩進部45により+1した歩進結果 $n+1$ と、ユーザから受信した認証用データ W_{n+1}, M_n と、及びメモリ43から読み出したデータ W_n とが一時的に保持されている。認証部60は、識別子Aを有するユーザから受信した識別子Aとデータ V_{n+1} とから $E(A, V_{n+1})$ を計算する一方向性関数部61と、計算したそのデータ W_{n+1} とメモリ43から識別子Aと対応して読み出したデータ W_n とを比較し、一致(OK)、不一致(NG)の比較結果OK/NGを出力する比較部62と、受信したデータ V_{n+1} とメモリ43から読み出したデータ W_n とからデータ M_{n+1} を計算する一方向性関数部63と、そのデータ M_{n+1} とメモリ43から読み出したデータ M_n とを比較し、一致、不一致の比較結果を出力する比較部64とから成る。制御部44は、比較部62及び64の出力が両方ともOKであれば、メモリ43に識別子Aと対応して保管されているユーザ宛のメールメッセージを読みだし、送受信部42からユーザに送出すると共に、レジスタ46に保持されているデータ n, W_n, W_{n+1}, M_n でメモリ43の識別子Aに対応して登録されているデータ W_{n+1}, W_n, M_n を書き換える。

【0052】図5に示したメールサーバ装置の機能構成におけるメモリ43、制御部44、歩進部45、レジスタ46、初期登録部50及び認証部60はコンピュータのソフトウェアとして実現される。即ち、メールサーバコンピュータは図3におけるメールサーバ側処理手順を実行するプログラムが記録された記録媒体を有してお

り、そのプログラムに従ってサーバ側の認証処理を実行する。

【0053】 上述の第1実施例において、一方向性変換をFEAL暗号方式で実現した場合、被認証者側の認証処理を0.6KByte程度（うち、FEALが0.4KByte）のプログラムで記述することができる。このように、この発明ではユーザは図1で示したCINONと同様に、認証処理において自分のパスワードSをメールサーバに送信しないので、インターネットを通した認証処理を安全に行うことができる。しかも、CINONで必要とされた乱数を使用しないので、乱数を記憶しておくためのICカードの様な記録媒体を必要とせず、また乱数生成機能、及びICカードへの読み書き機能を必要としない。また、乱数を使用しないので、それだけ認証処理のデータサイズが小さくてよい。従って、ホスト装置においては認証処理時間が短い。これは、この発明が処理能力の低いホスト装置とも使用可能であることを示している。

実施例2

上述の第1実施例では、この発明の認証方法をSMTP通信を使った電子メールでのユーザとメールサーバ間の認証手順に適用した場合を説明したが、ユーザがインターネット上でホストサーバによる各種サービスをHTTP通信を使って受ける場合における、ユーザとホスト間の認証手順にこの発明を適用してもよい。その場合の実施例を次ぎに説明するが、ここでは更に、ユーザ側の認証手順（プログラム）をホスト側からアプレットとして受信し、それを使う場合に付いて説明する。

【0054】 インターネット利用の高度化、多様化に対応して端末には各種プログラムを内蔵することなく、その端末の処理要求に応じて、その処理手順（プログラム）をその都度、その端末は相手（サーバ）から通信を介して送り込まれ、その送り込まれた処理手順をその端末が実行する方法が普及しようとしている。これは、インターネットにおいて、ユーザからの情報送受信要求があった時に、サーバ側が要求された処理手順を予め決められた言語、例えばJavaで記述された特定の通信単位、例えばAppletに埋め込んだものをユーザに送り込み、ユーザ側でその処理手順（プログラム）にもとづく処理が実行されるというもので、従来のOS（オペレーティングシステム）の概念を根底から変えてしまう画期的な方法である。今後、このような方法を用いる情報送受信が普及してくるに伴い、ユーザの認証機能がますます重要になってくる。第2の実施例は、この発明の認証方法をこのような手法環境へ適用するものである。

【0055】 なお、以下の説明に用いる記法は、これまでの説明に用いたものと同じである。以下の動作説明において、通信はHTTPで行われる。

<初期登録処理（図6）>ステップS1：ユーザ（被認証者）は、サーバ（認証者装置）に対して、初期登録要求を識別子（アカウント）Aと共に送る。

【0056】 ステップS2：サーバはこの要求に対応してユーザ識別子Aを登録する。

ステップS3：サーバは更に初期登録処理を記述した通信単位（Applet）をユーザに送付する。

ステップS4：この通信単位プログラムを受信したユーザは、ユーザ端末においてそのアプレットプログラムを使ってユーザ識別子A及びパスワードSを設定する。

【0057】 ステップS5：ユーザは更にアプレットプログラムを使って、以下の手順：

```

10   $V_0 = E(A, S)$ 
 $W_0 = E(A, V_0)$ 
 $V_1 = E(A, S(+1))$ 
 $W_1 = E(A, V_1)$ 
 $M_1 = E(W_1, V_0)$ 
 $n \leftarrow n + 1$ 

```

で、初期データ W_0 、 W_1 、 M_1 を算出する。

【0058】 ステップS6：ユーザは識別子Aと共にサーバ側へ送信する。 W_0 は回目の認証データ、 W_1 は次々回の認証データ、 M_1 は W_1 の正当性検証用データである。

ステップS7：サーバ側では、受信した識別子Aと対応させて、認証回数 n の初期値 $n=1$ 及び受信したデータ W_0 、 W_1 、 M_0 を登録する。

<認証処理および情報のやりとり（図7）>初期登録処理（図6におけるステップS7）の終了後、第 n 回目（ $n=1, 2, \dots$ ）の認証手順は以下の通りである。なお、この時点で、ホスト側には、既に、 n 、 W_{n-1} 、 W_n 、 M_{n-1} が登録されている。

ステップS1：ユーザは、まずサーバに対して、サービス起動の要求を送出すると共にユーザ識別子Aを通知する。

【0059】 ステップS2：サーバは出先にいるユーザからの、サービス起動要求とユーザ識別子Aを受信すると、認証処理Appletと、識別子Aに対応して登録されている認証回数 n とをユーザに返信する。

ステップS3：ユーザはサーバ側より、認証処理Appletと n の値を受け取り、アプレットプログラムに従って以下の手順：

```

 $V_{n-1} = E(A, S(+)(n-1))$ 
40  $V_n = E(A, S(+)(n))$ 
 $V_{n+1} = E(A, S(+)(n+1))$ 
 $W_{n-1} = E(A, V_{n-1})$ 
 $M_n = E(W_{n-1}, V_n)$ 

```

で認証用データ V_{n-1} 、 W_{n-1} 、 M_n を算出する。

【0060】 ステップS4：ユーザは更に、これらのデータ V_{n-1} 、 W_{n-1} 、 M_n 、及び送信したい情報がある場合にはその情報を、サーバに送付する。

ステップS5：サーバはユーザ側より送付されてきたデータ V_{n-1} 、 W_{n-1} 、 M_n により、以下の認証処理を行う。識別子Aと対応して登録されているデータ W_{n-1} と、受信し

たデータ V_{n-1} から計算した $E(A, V_{n-1})$ とを比較し、一致した場合、ユーザを正当とする。一致しない場合、そのユーザを不当とし、処理を終了する。

【0061】ユーザを正当とした場合、更に、登録されている M_{n-1} と $E(W_n, V_{n-1})$ を比較し、一致した場合、 W_n を正当とする。一致しない場合、 W_n を不当とし処理を終了する。

ステップS6：サーバはユーザ及び W_n の両方を正当と判定した場合、要求された情報送受信サービスの提供を開始する。

【0062】ステップS7：サーバは更に、現在登録してあるデータ W_{n-1} 、 W_n 、 M_{n-1} に換えて、 W_n 、 W_{n-1} 、 M_n を識別子Aに対応して新たに登録する。また、 n をインクリメントする。この実施例においても、実施例1の場合と同様に、一方向性関数 E をFEAL暗号方法で実現した場合、認証処理を0.6KByte程度（うち、FEALが0.4KByte）のプログラムで記述することができる。このサイズは、AppleIIプログラムを記述した場合、通信への負荷をほとんど生じさせない規模である。

【0063】実施例1では電子メールへこの発明を適用し、電子メールにより、出先端末の電子メール加入者の環境を一時的に借りてファイアウォールに影響されることなく、自己へのメッセージを受け取ることが可能であることを示し、実施例2においては通信プロトコル（HTTP）によりこの認証処理を行うことを示した。更に、これら両実施例を組み合わせ以下に説明する第3実施例のような形態も可能である。

実施例3

一般にインターネットは混雑していて、情報が円滑に送受信できない場合が多い。実施例1で示したように、ファイアウォールを回避するために認証情報を電子メールプロトコルでやりとりする場合、条件によっては数分間の時間を要する。この間、利用者に待機を強いるのはサービス上好ましくないと考えられる場合、図8に示すように、ユーザ端末14とメールサーバ13の間に中継サーバ18を設ける。メールサーバ13がファイアウォール12Fの内側、即ちイントラネット12の内部ネットワークにあるのに対して、この中継サーバ18は、インターネット11上にあり、外部に公開しているものとする。また、中継サーバ18はユーザに対する認証機能を持っているものとする。認証機能は従来提案されているどの様なものでもよいが、以下の説明では、この発明を適用した認証処理を行うものとする。メールサーバ13には前述した実施例1又は2の場合と同様に予めユーザが識別子Aに対応させてデータ $n=1$ 、 W_1 、 W_1 、 M_1 を初期登録しておく。又、ユーザと中継サーバ間の認証回数を n' で表すと、中継サーバにユーザの識別子Aと対応させてデータ $n'=1$ 、 W_1 、 W_1 、 M_1 を初期登録しておく。

【0064】第3実施例においては、インターネットに接続された端末14とイントラネット12に接続されたメ

ールサーバ13との通信は、中継サーバ18を介して行い、しかも、インターネット11に接続された端末14と中継サーバ18間はHTTPなどの高速転送プロトコルを用いて送受信を行い、中継サーバ18とメールサーバ13との間はSMTPのような電子メールプロトコルを使って通信を行う。

【0065】図9はこの様なシステムにおいて、ユーザが出先のインターネット端末14から n 回目にメールサーバ13に自分宛の電子メールを取りにいく場合の手順を示している。ただし、この時点でメールサーバ13には識別子Aに対応してデータ n 、 W_{n-1} 、 W_n 、 M_{n-1} が登録されており、中継サーバ18には識別子Aに対応してデータ n' 、 W_{n-1} 、 W_n 、 M_{n-1} が登録されている。

【0066】ステップS1：ユーザはインターネット11に接続された端末14からメール要求と、自分の識別子Aとを中継サーバ18に送る。

ステップS2：中継サーバ18は受信したメール要求と識別子Aを電子メールでメールサーバ13に送る。

ステップS3：メールサーバ13は受信した識別子Aに対応する認証回数 n を中継サーバ18に電子メールで送信し、

ステップS4：中継サーバ18はその認証回数 n をユーザに転送する。

【0067】ステップS5：ユーザは受信した認証回数 n を使って図3又は7のステップS3と同様の手順により認証用データ V_{n-1} 、 W_{n-1} 、 M_n を計算し、更に

ステップS6：ユーザはそれら認証用データを識別子A及びメール要求と共に中継サーバに送る。メール要求がメール送信の場合は、送信すべきメールメッセージも送る。ここで、ユーザは一旦、中継サーバ18との接続を切断し、必要に応じて他のタスクを実行する。

【0068】ステップS7：中継サーバ18は受信した識別子A、メール要求（及び送信すべきメッセージ）、認証用データ V_{n-1} 、 W_{n-1} 、 M_n を電子メールによりメールサーバ13に転送する。

ステップS8：メールサーバ13は受信した識別子Aに対応して登録されているデータ W_{n-1} 、 W_n 、 M_{n-1} を読みだし、図3又は7のステップS5と同様の手順により、受信した V_{n-1} の正当性と次回 $n+1$ の認証に使用する W_n の正当性を認証する。これら2つが正当であると判定されると、

ステップS9：メールサーバは識別子Aに対応するユーザ宛のメールメッセージを中継サーバに転送し、或いは、送信すべきメッセージを送出し、送出確認情報を中継サーバに送る。更に、

ステップS10：メールサーバは登録されているデータ W_{n-1} 、 W_n 、 M_{n-1} を W_n 、 W_{n-1} 、 M_n に書き換えると共に、 n をインクリメントする。

【0069】ステップS11：中継サーバは受信した識別子A宛の電子メールメッセージ及び／又は送信確認情

報を識別子 A に対応して保管する。

ステップ S 12 : ユーザは中継サーバとの接続を切断して数分経過した後、任意の時間に中継サーバに識別子 A とメール要求を送る。

ステップ S 13 : 中継サーバは識別子 A に対応して登録してある認証回数 n' を読みだし、ユーザに送る。

【0070】ステップ S 14 : ユーザは受信した n' を使って図 3 又は 7 のステップ S 3 と同様の手順で認証用データ $V_{n'}$, $W_{n'}$, $M_{n'}$ を計算し、

ステップ S 15 : ユーザはそれらの中継サーバに送る。 10

ステップ S 16 : 中継サーバは受信したデータ $V_{n'}$, $W_{n'}$, $M_{n'}$ から図 3 又は 7 のステップ S 5 と同様の手順で $V_{n'}$ と $W_{n'}$ の正当性を認証し、それによってメールを要求しているユーザが正当なユーザであると判定し、ステップ S 17 : 中継サーバは識別子 A に対応して保管してある電子メールメッセージをユーザに転送する。更に、

$$\begin{aligned} V_0 &= E(A(+)A_n, S) & (1a') \\ W_0 &= E(A(+)A_n, V_0) & (1b') \\ V_1 &= E(A(+)A_n, S(+)1) & (1c') \\ W_1 &= E(A(+)A_n, V_1) & (1d') \\ M_0 &= E(W_1, V_0) & (1e') \end{aligned}$$

及び

$$\begin{aligned} V_{n-1} &= E(A(+)A_n, S(+) (n-1)) & (2a') \\ V_n &= E(A(+)A_n, S(+)n) & (2b') \\ V_{n+1} &= E(A(+)A_n, S(+) (n+1)) & (2c') \\ W_{n-1} &= E(A(+)A_n, V_{n-1}) & (2d') \\ M_n &= E(W_{n-1}, V_n) & (2e') \end{aligned}$$

のように、識別子 A の代わりに $A(+)A_n$ を使い、メールサーバの認証ステップ S 8 において $W_{n-1}=E(A(+)A_n, V_{n-1})$ 30 の一致と、 $M_{n-1}=E(W_{n-1}, V_n)$ の一致を検証する。同様

$$\begin{aligned} V_0 &= E(A(+)A_n, S) & (1a'') \\ W_0 &= E(A(+)A_n, V_0) & (1b'') \\ V_1 &= E(A(+)A_n, S(+)1) & (1c'') \\ W_1 &= E(A(+)A_n, V_1) & (1d'') \\ M_0 &= E(W_1, V_0) & (1e'') \end{aligned}$$

及び

$$\begin{aligned} V_{n'-1} &= E(A(+)A_n, S(+) (n'-1)) & (2a'') \\ V_{n'} &= E(A(+)A_n, S(+)n') & (2b'') \\ V_{n'+1} &= E(A(+)A_n, S(+) (n'+1)) & (2c'') \\ W_{n'-1} &= E(A(+)A_n, V_{n'-1}) & (2d'') \\ M_{n'} &= E(W_{n'-1}, V_{n'}) & (2e'') \end{aligned}$$

のように $A(+)A_n$ を使い、中継サーバによる認証ステップ S 16 において $W_{n'-1}=E(A(+)A_n, V_{n'-1})$ の一致と $M_{n'-1}=E(W_{n'-1}, V_{n'})$ の一致を検証する。この方法によれば、ユーザは安全性を損なわずに同じパスワード S と識別子 A を、メールサーバとの認証処理及び中継サーバとの認証処理のどちらにも使用できるので都合がよい。

【0072】この様に、図 9 の実施例では、ユーザがステップ S 6 でメールサーバ 13 に対しメール要求を送つ

ステップ S 18 : 中継サーバは登録されているデータ $W_{n'-1}$, $W_{n'}$, $M_{n'}$ を $W_{n'-1}$, $W_{n'}$, $M_{n'}$ に書き換え、 n' をインクリメントする。

【0071】この例では、簡単のため、ステップ S 14 における認証用データの計算に使用する識別子 A とパスワード S はメールサーバとの間の認証処理で使用するものと同じものを使用する場合を示しているが、パスワードは異なるパスワード S' を使ってもよい。その場合、中継サーバに予め登録するデータ W_0 , W_1 , M_0 も、 S' を使って求めたものである。或いは、ユーザは中継サーバとの認証処理に、メールサーバとの認証処理と同じパスワード S と識別子 A を使用し、以下のような処理を行ってもよい。予めメールサーバ及び中継サーバの公開された識別子をそれぞれ A_n 及び A_n とすると、ユーザとメールサーバ間の認証処理においては、前述の初期登録のための式 (1a) ~ (1e) 及び検証のための式 (2a) ~ (2e) において、次式

に、ユーザと中継サーバ間の認証処理においては、前述の初期登録のための式 (1a) ~ (1e) 及び検証のための式 (2a) ~ (2e) における各識別子 A の代わりに、次式

$$\begin{aligned} (1a'') & \\ (1b'') & \\ (1c'') & \\ (1d'') & \\ (1e'') & \end{aligned}$$

てから、中継サーバ 18 との接続を切断し、他のタスクに切り替えることができる。要求したメールは中継サーバとの接続切断後、数分経過してからであればいつでも中継サーバに取りにいくことができる。従って、ステップ S 6 のメール要求からメールサーバで認証 (ステップ S 8) 後、メールが中継サーバに転送されてくるまで通信を接続したままで待機する必要はない。

【0073】図 9 の実施例では、第 1 及び第 2 実施例の

場合と同様に、ユーザとメールサーバ13間の認証回数 n はメールサーバ13から与えられる場合を示した。しかしながら、図9において中継サーバが識別子Aに対応して認証回数 n と n' の両方を持っていれば、ステップS2、S3を省略することができる。その場合の、 n 回目の認証処理を図10に示す。

【0074】図10の例では、メールサーバは初期登録されたデータのうち、認証回数初期値 $n=1$ を予め中継サーバに送付しておく。中継サーバには、図9の場合と同様に識別子Aと対応させて n' 、 W_{n-1} 、 W_n 、 M_{n-1} が登録されており、更に、ユーザとメールサーバ間の認証回数 n も中継サーバには識別子Aと対応させて登録されている。

【0075】ステップS1でユーザから識別子Aとメール要求を受けると、中継サーバはメールサーバにそのメール要求と識別子Aを転送せず、ステップS2で直ちに識別子Aと対応する認証回数 n をユーザに返送する。従って、ユーザは、 n を使ってステップS3で認証用データ V_{n-1} 、 W_{n-1} 、 M_n を計算し、ステップS4でこれら認証用データを識別子A及びメール要求と共に中継サーバを介してメールサーバに送り、その後、中継サーバとの接続を切断して、端末を他のタスクに切り替えることができる。ステップS4～S15は、図9におけるステップS6～S17と全く同様である。中継サーバはステップS16で認証用データ W_{n-1} 、 W_n 、 M_{n-1} を W_{n-1} 、 W_n 、 M_n に書き換え、中継サーバの認証回数 n' 及びメールサーバの認証回数 n をそれぞれインクリメントする。なお、認証回数 n のインクリメントは、ステップS7でメールサーバから認証されたことを表す情報を受けた後であればいつ行ってもよい。

【0076】図10の実施例においても、図9で説明したと同様に、ユーザとメールサーバ間の認証処理には、識別子Aの代わりに $A(+)$ A_n を使い、ユーザと中継サーバ間の認証には、 A の代わりに $A(+)$ A_n を使うのが好ましい。この様に、図9及び10の実施例では、ユーザは中継サーバ18を用いてサービス要求とユーザ識別子Aを中継サーバ18に送信することにより認証手順を起動した後、一旦中継サーバとの接続を切断する。中継サーバ18は、ユーザから送られてきた認証用データを用いて認証者装置であるメールサーバに送り、認証処理を行い、OKであれば電子メールの転送を受ける。ユーザは、しばらくして再度中継サーバと認証処理を行い、必要な情報の転送を得ることができる。

【0077】このような構成をとることによって、ユーザと中継サーバ間では、中継サーバが公開されているために、HTTPなどの高速転送プロトコルを用いることができる。また、中継サーバとイントラネット内部にあるメールサーバ間の通信も、ファイアウォールを回避するために電子メールプロトコルを用いるとはいえ、経由するホスト数が少ないため、転送速度を高めることができる。

【0078】また、更に高速処理を実現するために、認証に用いている認証回数 n を、メールサーバと中継サーバで共有するようにし、認証の度毎に同期をとって更新するようにすれば、認証手順を1往復削減できる。

実施例4

次に、この発明の認証方法を、インターネット上でのサービスに対する課金システムに適用した実施例を、図11、12を参照して説明する。近年、インターネット上でのショッピングが実現化されていくことが予想されている。これまでのインターネットショッピングでは、ユーザはインターネット上のサービスプロバイダのホームページにアクセスし、所望の商品やサービスに対し、クレジットカードでの支払いを行うのが一般である。しかしながら、クレジットカードでの支払いは1回で使用可能な最低限の金額が比較的に大きく、日常的に利用するには不便である。しかも、利用者はクレジットカードの番号をプロバイダに送信する必要があるので、安全上問題がある。

【0079】不特定多数のユーザは、それぞれが決めた金額 $\$X$ をインターネット上に設けられた課金管理センタ21に対し、例えば、電話などを用いて、まとめてクレジットカードで支払う。或いは、ダイヤルQ2（料金代行徴収サービス）により支払うなどの方法により、それぞれ異なるパスワードSとアカウントAの組が例えば郵送、或いは直接電話からメッセージで与えられる。ステップS0：課金管理センタは、各アカウントAに対して支払われた金額 X と、この発明による認証手順に使われる初期登録データ $n=1$ 、 W_0 、 W_1 、 M_0 をメモリ（図示せず）に保持しておく。

【0080】ステップS1：ユーザは、インターネット上のサービスプロバイダ22のホームページなどからサービスカタログを得て、所望のサービスを指定するサービス要求信号とアカウントAをサービスプロバイダに送信する。

ステップS2：サービスプロバイダはユーザのアカウントAを課金管理センタに送り、対応する認証回数 n を要求する。

【0081】ステップS3：センタはアカウントAに対応する認証回数 n をメモリから読み出し、サービスプロバイダに送る。

ステップS4：プロバイダはJava Applet で記述されたユーザ側認証手順のプログラムと共に、認証回数 n をユーザに送る。

ステップS5：ユーザはパスワードS、アカウントA、認証回数 n を使って認証手順に従って式(2a)～(2e)を計算し、認証用データ V_{n-1} 、 W_{n-1} 、 M_n を求め、ステップS6でサービスプロバイダに送る。

【0082】ステップS7：プロバイダはユーザが指定したサービスの金額 x と、プロバイダのアカウント A_n と共に、認証用データ V_{n-1} 、 W_{n-1} 、 M_n 及びユーザアカウン

トAを課金管理センタに転送する。

ステップS8: センタは支払金額xがユーザアカウントAに対応する残額X以下であるかを判定し、以下であれば図3のステップS5と同様に、受信したデータ V_{n-1} の正当性及び登録されているデータ W_n の正当性を検証し、これらが正しければ、ステップS9で確認信号OKをプロバイダに送信する。

【0083】ステップS10: センタは更に、登録データを W_n, W_{n+1}, M_n に更新し、認証回数nをインクリメントし、ユーザの残額Xを $X-x$ に更新する。又、プロバイダのアカウントA_rの残額 X_r を X_r+x に更新する。

ステップS11: サービスプロバイダは、センタからの確認信号OKを受信すると、ユーザに指定されたサービスを提供する。

【0084】この様に、この発明の認証手順をインターネットショッピングにおける認証に適用することにより、少額な支払いも可能となり、しかも安全に決済を行うことができる。

【0085】

【発明の効果】以上説明したように、この発明の情報送受信制御方法は、その認証手順において、被認証側にICカード等の記憶媒体の読み書きを行う機構や乱数発生機構を必要とせず、小さいプログラムサイズでの処理を可能にしているため、インターネット家電のような処理能力の限られた端末に対しても、安全な情報蓄積検索サービスを提供することが可能になる。

【図1】

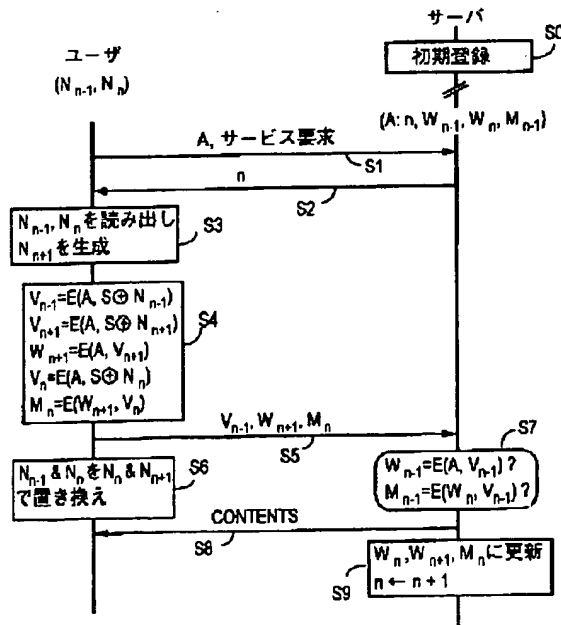


図1

【図面の簡単な説明】

【図1】従来のCINONの認証手順を示す図。

【図2】この発明の第1の実施例である公衆電子メール転送サービスのシステムの概要を示す図。

【図3】第1の実施例である公衆電子メール転送プロトコルの詳細を示す図。

【図4】第1実施例におけるユーザ端末の機能ブロック図。

【図5】第1実施例におけるメールサーバの機能ブロック図。

【図6】サーバからJavaのAppletを使って提供される認証手順を使って認証手順を実行する場合にこの発明を適用した場合の初期登録手順を示すフロー図。

【図7】第2実施例におけるn回目の認証手順を示すフロー図。

【図8】インターネット上の中継サーバを介してメールサーバにアクセスする場合にこの発明を適用した第3実施例のシステム図。

【図9】図8のシステムにおいて、第3実施例による認証手順を示すフロー図。

【図10】第3実施例の変形実施例を示すフロー図。

【図11】この発明による認証方法をインターネットショッピングに適用した場合のシステム図。

【図12】この発明の認証方法が適用されたインターネットショッピングの手順を示す流れ図。

【図3】

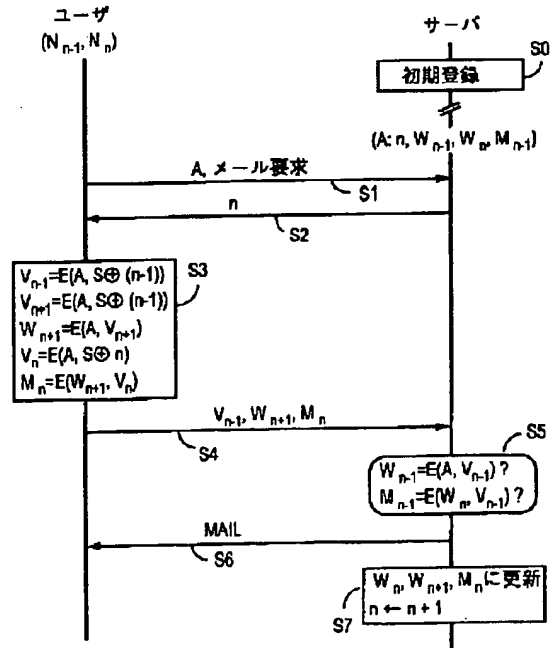


図3

【図 2】

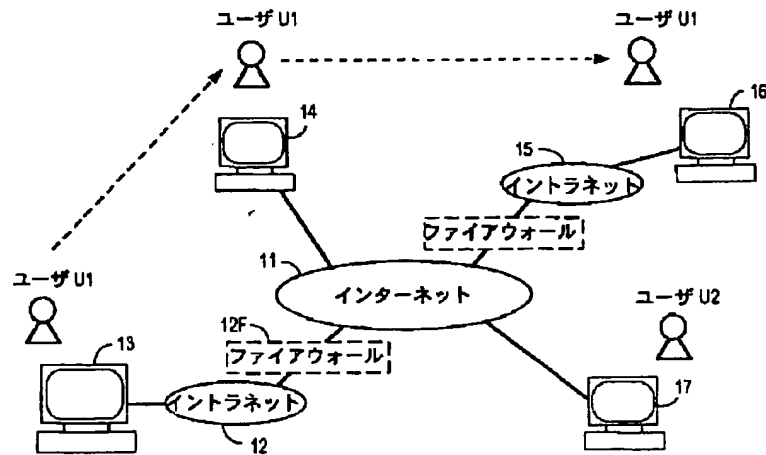


図 2

【図 4】

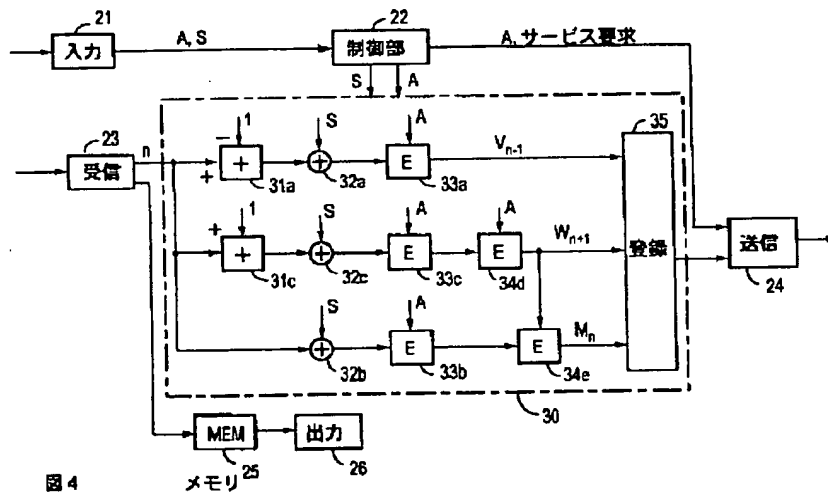


図 4

【図 8】

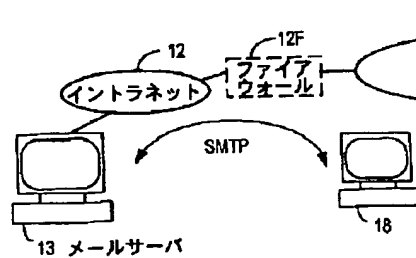


図 8

【図 11】

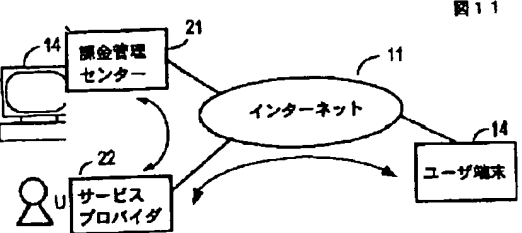


図 11

【図 5】

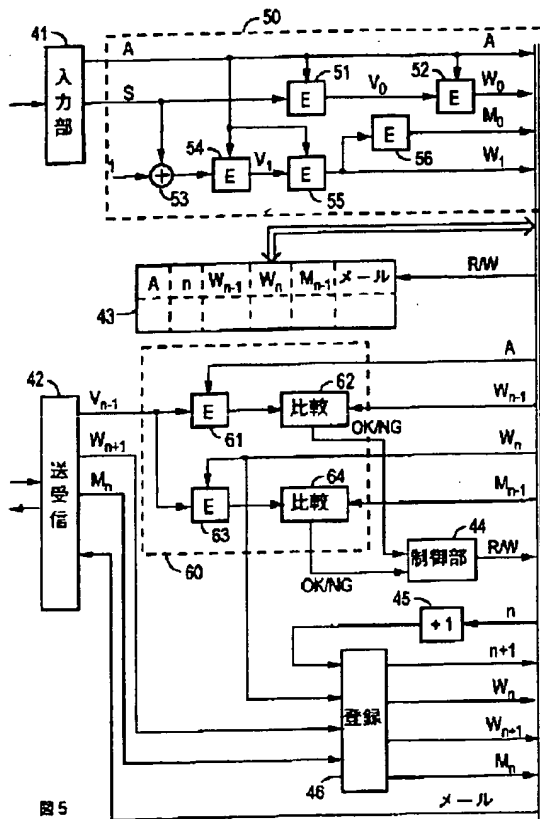


図 5

【図 7】

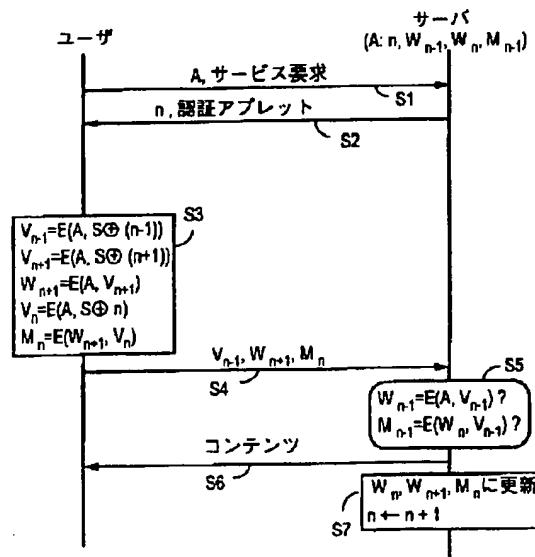


図 7

【図 6】

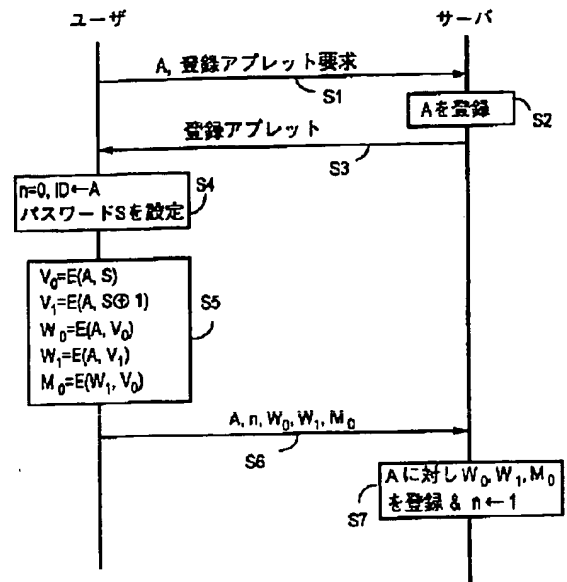


図 6

【図 9】

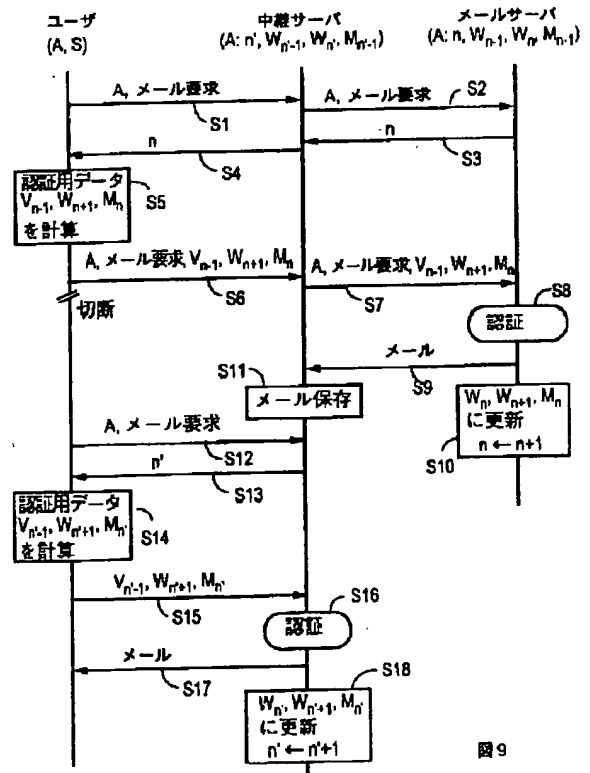


図 9

【 図 1 0 】

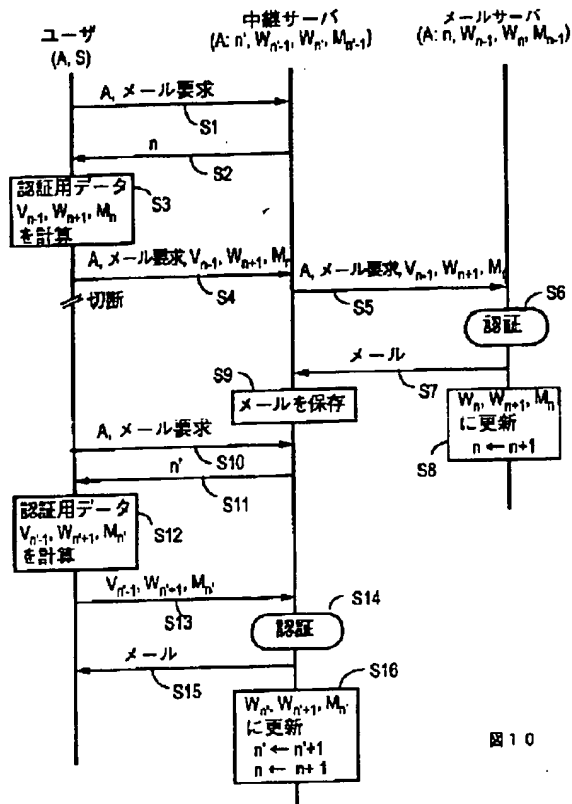


図 1 0

【 図 1 2 】

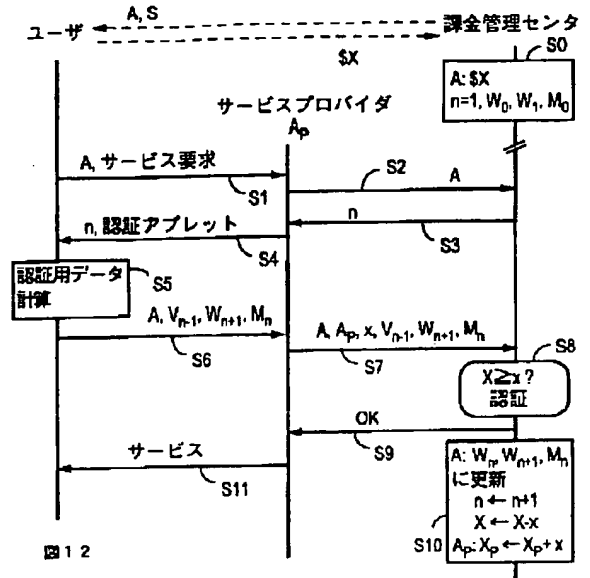


図 1 2